

# RISK TO HOMELAND SECURITY FROM IDENTITY FRAUD AND IDENTITY THEFT

---

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON IMMIGRATION,  
BORDER SECURITY, AND CLAIMS

AND THE

SUBCOMMITTEE ON CRIME, TERRORISM,  
AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY  
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

---

JUNE 25, 2002

---

**Serial No. 86**

---

Printed for the use of the Committee on the Judiciary



Available via the World Wide Web: <http://www.house.gov/judiciary>

---

U.S. GOVERNMENT PRINTING OFFICE

80-452 PDF

WASHINGTON : 2002

---

For sale by the Superintendent of Documents, U.S. Government Printing Office  
Internet: [bookstore.gpo.gov](http://bookstore.gpo.gov) Phone: toll free (866) 512-1800; DC area (202) 512-1800  
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

## COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., WISCONSIN, *Chairman*

HENRY J. HYDE, Illinois	JOHN CONYERS, JR., Michigan
GEORGE W. GEKAS, Pennsylvania	BARNEY FRANK, Massachusetts
HOWARD COBLE, North Carolina	HOWARD L. BERMAN, California
LAMAR SMITH, Texas	RICK BOUCHER, Virginia
ELTON GALLEGLY, California	JERROLD NADLER, New York
BOB GOODLATTE, Virginia	ROBERT C. SCOTT, Virginia
STEVE CHABOT, Ohio	MELVIN L. WATT, North Carolina
BOB BARR, Georgia	ZOE LOFGREN, California
WILLIAM L. JENKINS, Tennessee	SHEILA JACKSON LEE, Texas
CHRIS CANNON, Utah	MAXINE WATERS, California
LINDSEY O. GRAHAM, South Carolina	MARTIN T. MEEHAN, Massachusetts
SPENCER BACHUS, Alabama	WILLIAM D. DELAHUNT, Massachusetts
JOHN N. HOSTETTLER, Indiana	ROBERT WEXLER, Florida
MARK GREEN, Wisconsin	TAMMY BALDWIN, Wisconsin
RIC KELLER, Florida	ANTHONY D. WEINER, New York
DARRELL E. ISSA, California	ADAM B. SCHIFF, California
MELISSA A. HART, Pennsylvania	
JEFF FLAKE, Arizona	
MIKE PENCE, Indiana	
J. RANDY FORBES, Virginia	

PHILIP G. KIKO, *Chief of Staff-General Counsel*

PERRY H. APELBAUM, *Minority Chief Counsel*

---

## SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

GEORGE W. GEKAS, Pennsylvania, *Chairman*

DARRELL E. ISSA, California	SHEILA JACKSON LEE, Texas
MELISSA A. HART, Pennsylvania	BARNEY FRANK, Massachusetts
LAMAR SMITH, Texas	HOWARD L. BERMAN, California
ELTON GALLEGLY, California	ZOE LOFGREN, California
CHRIS CANNON, Utah, <i>Vice Chair</i>	MARTIN T. MEEHAN, Massachusetts
JEFF FLAKE, Arizona	
J. RANDY FORBES, Virginia	

GEORGE FISHMAN, *Chief Counsel*

LORA RIES, *Counsel*

ART ARTHUR, *Full Committee Counsel*

CINDY BLACKSTON, *Professional Staff*

LEON BUCK, *Minority Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

LAMAR SMITH, Texas, *Chairman*

MARK GREEN, Wisconsin, *Vice Chair*

HOWARD COBLE, North Carolina

BOB GOODLATTE, Virginia

STEVE CHABOT, Ohio

BOB BARR, Georgia

RIC KELLER, Florida

MIKE PENCE, Indiana

ROBERT C. SCOTT, Virginia

SHEILA JACKSON LEE, Texas

MARTIN T. MEEHAN, Massachusetts

WILLIAM D. DELAHUNT, Massachusetts

ADAM B. SCHIFF, California

JAY APPERSON, *Chief Counsel*

SEAN McLAUGHLIN, *Counsel*

ELIZABETH SOKUL, *Counsel*

KATY CROOKS, *Counsel*

ERIC HULTMAN, *Full Committee Counsel*

BOBBY VASSAR, *Minority Counsel*



# CONTENTS

JUNE 25, 2002

## OPENING STATEMENT

	Page
The Honorable George W. Gekas, a Representative in Congress From the State of Pennsylvania, and Chairman, Subcommittee on Immigration, Border Security, and Claims .....	1
The Honorable Lamar Smith, a Representative in Congress From the State of Texas, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security .....	2
The Honorable Robert C. Scott, a Representative in Congress From the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security .....	3
The Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Immigration, Border Security, and Claims .....	5

## WITNESSES

Mr. Paul J. McNulty, United States Attorney, Eastern District of Virginia	
Oral Testimony .....	7
Prepared Statement .....	9
Mr. James G. Huse, Jr., Inspector General, Social Security Administration	
Oral Testimony .....	13
Prepared Statement .....	14
Mr. Richard M. Stana, Director, Administration of Justice Issues, United States General Accounting Office	
Oral Testimony .....	20
Prepared Statement .....	22
Mr. Edmund Mierzwinski, Consumer Program Director, State Public Interest Research Groups	
Oral Testimony .....	37
Prepared Statement .....	38

## LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress From the State of Texas, and Ranking Member, Subcommittee on Immigration, Border Security, and Claims .....	6
--	---

## APPENDIX

### MATERIAL SUBMITTED FOR THE HEARING RECORD

Letter to Ms. Jackson Lee from Mr. Huse, Inspector General, Social Security Administration .....	61
Prepared Statement of the Honorable Zoe Lofgren with attached testimony from Linda Foley, Executive Director, Identify Theft Resource Center .....	64



## **RISK TO HOMELAND SECURITY FROM IDENTITY FRAUD AND IDENTITY THEFT**

**TUESDAY, JUNE 25, 2002**

HOUSE OF REPRESENTATIVES,  
SUBCOMMITTEE ON IMMIGRATION,  
BORDER SECURITY, AND CLAIMS,  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.*

The Subcommittees met jointly, pursuant to notice, at 4 p.m., in Room 2141, Rayburn House Office Building, Hon. George W. Gekas [Chairman of the Subcommittee on Crime, Terrorism, and Homeland Security] presiding.

Mr. GEKAS. The hour of 4 o'clock having arrived, this special joint hearing will come to order.

The joint hearing is, of course, composed of the two Subcommittees in the Judiciary Committee which have oversight capacity on a variety of mutual issues but on this one in particular. It is composed, of course, of the Subcommittee on Immigration, Border Security, and Claims and the Subcommittee on Crime, Terrorism, and Homeland Security, the Chairman of which is Lamar Smith of Texas, who joins us and who helps us constitute the hearing quorum for the purpose of this hearing.

As the other Members appear in an order which the staff will maintain, we will recognize them as the need arises, but we plan to forge ahead with the hearing and will accord all the Members the right to insert statements in the record and to other—and we will otherwise accommodate them as they appear.

The series of problems that have led to this hearing, of course, has to do with identity fraud, and that takes—takes characterization from many different sources, but the one that most disturbs us is the identity fraud that's identified with Social Security identification. And we know, for instance, that our distinguished former—I don't even know what to call him anymore—Paul McNulty. I was remarking to him at the start that I think this is his eighth title since I've known him. But we welcome him. But he is the one who has outlined some of the problems in the airports, which we will discuss, having to do with this very same subject.

So we will be inclined to worry with you on the existence of the problems and to work through whatever recommendations that we can fashion together to try to limit the damage that has been done and will still be done if we do not take complete hold of the entire situation.

So we will begin the questioning of the witnesses after we accord the time to the gentleman from Texas, Mr. Smith, for an opening statement.

Mr. SMITH. Thank you, Mr. Chairman, and like you, I look forward to this joint hearing on identify fraud in all different variations.

Before I make any formal remarks, also like the Chairman, I'd like to single out Paul McNulty, who I consider to be a personal friend and who served as general counsel of the Crime Subcommittee before he went on to other green pastures. So, Paul, without slighting the rest of the witnesses who are here, I'm looking forward to hearing your testimony as well.

I'd also like to mention Roger Estes. Roger Estes is a police detective in Arlington County who went to great lengths to bring to our attention the problems with identity theft and identify fraud that we're talking about today. Mr. Estes, we are pleased to have you in the audience as well, and thank you for taking the initiative and alerting us to so many of the problems involved.

Mr. Chairman, since last September, it has become even more apparent how crucial it is to have accurate information regarding an individual's identity. Even without the threat of terrorism, this would be a serious issue. Identity theft and fraud cost businesses and individuals time, money, and sometimes their lives.

There are three documents frequently used to establish false identities that must be made more secure. We can do a great deal to protect our homeland security if we tighten up the laws governing issuing of driver's licenses, Social Security cards, and birth certificates.

Many of us were shocked to hear how easy it was for members of al-Qaeda to obtain driver's licenses in three different States that allowed them onto U.S. airlines on September 11. Problems identity fraud are not unique to these States. Each State has different standards for driver's licenses. Some even allow illegal aliens to obtain driver's licenses.

In addition, each State has different laws regarding what documents may be used to prove identity or residency to obtain a driver's license. The problem is not only with individuals obtaining false driver's licenses. Identification procedures are full of loopholes that make it easy for criminals to take advantage of the system.

Many of the September 11 terrorists also obtained fraudulent Social Security cards or numbers through theft of legitimate Social Security numbers of others or through the use of counterfeit documents. While it has become increasingly obvious in the past few years that identity theft can cause financial damage, it is now becoming apparent that it can cause damage of a much more serious nature.

Individuals can obtain fraudulent Social Security cards by inventing a number, stealing an existing Social Security card, buying a counterfeit card, obtaining counterfeit documents such as passports, birth certificates, or INS papers, or by fraudulently obtaining a valid replacement Social Security card.

The Social Security Administration is responsible for preventing some of this fraud, but weaknesses in the system make it difficult to detect in all cases.



In 1996, Congress ordered the Social Security Administration to develop a proposal for a Social Security card to provide individuals with proof of citizenship or proof of legal resident status that would be harder to counterfeit and harder to alter. Several different types of cards were developed in response to this request, but no action has been taken to implement the use of these new cards. And I know we have a witness who will be talking about that problem a little bit more.

Much of the fraud in both the Social Security system and driver's licensing systems is related to fraudulent birth certificates. Because these records are kept in many places by local registrars and there is no national standard for these documents, it is easy to create counterfeit birth certificates or alter legitimate certificates as well.

We look forward to hearing suggestions from our witnesses today on how Congress can better protect our citizens and how we can better address these problems.

Thank you, Mr. Chairman.

Mr. GEKAS. We thank the gentleman, and we acknowledge for the record the presence of the gentleman from Virginia, Mr. Scott, and we accord to him at this moment the right to make an opening statement.

Mr. SCOTT. Thank you, Mr. Chairman. The problem of identity theft has grown rapidly with the growth of automation and now is entrenched as a front-line issue in the war on terrorism. Nearly all of the September 11 hijackers obtained false documentation that allowed them to base themselves here in the United States while plotting the terrorist attacks. However, the war on terror has only added a second tier to an already serious problem with consumer-related identity theft. The threat posed by identity theft to homeland security as well as the dangerous economic and personal effects of consumer-related identity theft require immediate attention from the Government, law enforcement agencies, and the credit industry.

According to several sources, in May of 2000, there are two major forms of identity theft. True name fraud is when a perpetrator uses a consumer's personal information, often in the form of a Social Security card, to open new accounts in the consumer's name. Of the victims who responded to the survey, 76 percent were victims of this sort of fraud, with an average number of six new accounts being opened per victim.

Account takeover fraud occurs when perpetrators gain access to a consumer's existing accounts and make fraudulent charges. Victims of this type of fraud were faced with an average of \$6,000 worth of fraudulent charges. However, many victims indicated that in addition to financial stress, the personal stress, emotional trauma, and difficulty in repairing a damaged credit reputation were perhaps the most damaging.

Other types of identity theft include Social Security fraud, the use of a false Social Security number in tandem with a false or stolen identity, and so-called bust-out schemes where perpetrators use credit card terminals obtained by a shell or front business, can make charges to fraudulently obtain credit cards.

Identity theft victimizes between 500,000 and 700,000 victims each year, and all indications are that this number is rising. In March 2002, a GAO study reported a 40-percent increase in identity thefts reported to Social Security during a 7-month period in 2002 and over the same period in 2000. This documented increase does not take—even take into account the fact that many individuals are not even aware that they have been victimized until months after the fact and that some choose not to report such incidences to law enforcement agencies or identity theft hotlines.

Many States have begun to tackle these pressing problems. In Virginia, the Attorney General has created a task force to address economic crime—electronic crimes, including identity theft. The Federal Government needs to be ready to assist these types of efforts in any possible way. Tighter administration of Social Security cards and other Federal IDs are one effort to address identity theft, and we must develop these kinds of efforts to help drive the burgeoning market in illegal information.

I look forward to the testimony of our witnesses on how we can better address the growing problem of identity theft, and I'd like to particularly welcome the U.S. Attorney from my district, Paul McNulty, to testify before us today.

Thank you.

Mr. GEKAS. We thank the gentleman.

We'll proceed with introductions of the witnesses. Our first witness is, as aforesaid, Paul J. McNulty, the United States Attorney for the Eastern District of Virginia. Mr. McNulty has had more than 20 years of experience in Federal and State Government, most of which has involved law enforcement and criminal justice policy. Mr. McNulty's experience also includes over 12 years in the United States Congress where he was chief counsel and director of legislative operations for the majority leader of the U.S. House of Representatives, and for 8 years he served with the House Subcommittee on Crime, first as minority counsel and later as the chief counsel.

During those years he was a principal draftsman of many Federal anti-terrorism, drug-control, firearms, and anti-fraud statutes. Mr. McNulty is Chairman of the Washington/Baltimore High Intensity Drug Trafficking Area Task Force and is Vice Chairman of the Attorney General Ashcroft's Advisory Committee.

Next to him at the witness table is James G. Huse, Jr. He is the Inspector General of the Social Security Administration. Prior to his Social Security appointment, Mr. Huse was a special agent in the United States Secret Service for 25 years, rising to the position of assistant director. During his Secret Service career, he was also assigned as the liaison officer to the Department of Justice and to protective duties at the White House and many Presidential election campaigns. In 1995, he received a special award from the Secretary of the Treasury for his work as the Secret Service official in charge of the White House Security Review.

Next to him is, well known to Members of this Committee, Richard M. Stana, the Director for Justice Issues at the U.S. General Accounting Office. He has testified on behalf of the GAO before the Immigration Subcommittee and before the Judiciary Committee as a whole many times over the years. During his 26-year career with

the GAO, he has directed reviews on a wide variety of complex military and domestic issues in headquarters, field, and overseas offices. Most recently, he has directed GAO's work relating to law enforcement, drug control, immigration, corrections, court administration, and election systems.

They are joined as in the final seat, the fourth witness, Edward Mierzwinski, the Consumer Program Director, State Public Interest Research Groups. He has been a consumer advocate with U.S. PIRG, the national lobbying office for State PRGs, since January 1989. These are non-profit, non-partisan public interest advocacy organizations with offices around the country. Ed Mierzwinski has authored numerous reports on consumer, privacy, credit card, credit reporting, and other bank and financial issues. He is also often quoted in the national press and has appeared on shows including ABC's "Nightline," CNN's "Crossfire," NBC's "Today," and NPR's "Talk of the Nation." From 1993 through 1995, he was a member of the Federal Reserve Board of Governors Consumer Advisory Council.

We will begin with the testimony of the witnesses after we accord the lady from Texas, Ms. Lee, an opportunity for an opening statement.

MS. JACKSON LEE. Mr. Chairman, thank you very much, and I do thank you and the Chairman of the Subcommittee on Crime, Terrorism, and Homeland Security for holding this hearing, and I acknowledge the Ranking Member of the Crime Subcommittee.

This is a very important combined hearing inasmuch as it relates to the jurisdiction of both of our Committees, the Crime Subcommittee and the Immigration and Claims Committee. You would wonder, as you review September 11, how much of the ability of the terrorists to enter into this country had a lot to do with identity fraud and theft and how much prospectively we can expect creative individuals who wish to do evil that will be taking advantage of the flexibility and the freedom of this Nation in terms of identity fraud and theft.

Already identity fraud and theft is an enormous burden on our economy as it relates to our own citizens. In my own community, I have had a number of constituents who have been drastically impacted, negatively impacted, losing large sums of resources, because someone has taken advantage of their particular identity, and, I might say, their good name. And so the expertise that is before us this afternoon is key.

One of the issues that we confront, those of us who are here in the United States Congress, is that we will spend a lot of time in hearings dealing with practicalities. We are the practitioners, and my delay was because I was in a Science Committee hearing on cyber terrorism and how we can enhance science and technology to protect us against terrorism.

Well, we need the thinkers as well to be able to help us design the legislation that will be helpful in this new climate. And so I would hope that as we listen to the witnesses, what we will find is a way to balance the freedom of this country, the first amendment, the protection of the Constitution, the ability to protect without isolating or discriminating against particular groups, the ability to recognize names, if you will, as not names equaling ter-

rorism, but as they are intent on committing crimes, that these names do not signal to us that one group versus another is a terrorist group. But we'll be able to discern the actual facts and be able to present these facts so that legislation can be written.

I look forward to listening to the witnesses and, Messrs. Chairmen, I would ask that the entirety of my statement be submitted into the record as we proceed. And I thank you.

Mr. GEKAS. Without objection, the statement will be entered into the record.

[The prepared statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF THE HONORABLE SHEILA JACKSON LEE, A REPRESENTATIVE  
IN CONGRESS FROM THE STATE OF TEXAS

Good Afternoon Mr. Chairman. On September 11, the United States experienced the worst attack on its soil since World War II. An estimated 3000 people were killed in an attack on the World Trade Center in New York City. In the weeks following the attack, the U.S. government initiated a nationwide investigation into the reasons behind the failure of U.S. police and intelligence agencies to uncover the plot to destroy the Trade Center. In *Washington Post* stories earlier this year it was revealed that some of the September 11, 2001, hijackers had used identity theft and fraud to obtain false social security numbers and other identification documents to facilitate training and preparation for the September 11, attacks.

First, let me emphasize that I, like you, condemn fraud and its negative impact. None of us would approve of the fraudulent use of identification cards or any other documentation. People who fraudulently use identification documents can and should be punished. This is being done now. An alien at our border who has engaged in document fraud is inadmissible under section 212(a)(6)(C) of the INA. If the alien is in the United States already, he or she is deportable for document fraud under section 237(a)(3)(C) of the INA. In addition, it is unlawful for any person to forge, counterfeit, alter or falsely make any document for immigration related purposes.

Efforts at stopping terrorism beg the question at which point is it best to stop the terrorist. Clearly, the best point to stop terrorists is prior to their entry into the country, before they have access to our social security administration, departments of motor vehicles and other infrastructure critical to secure identification documents. During testimony before the House Committee on Small Business, last week, Immigration and Naturalization Service (INS) Commissioner James Ziglar pointed out that "18 of the 19 hijackers entered the United States on visitors visas." He further explained that "[t]hey made concerted efforts to do so, it is logical to assume, because that made them less likely to come to the attention of federal authorities." This glaring fact underscores the difficulties faced by agencies in preventing terrorists from obtaining fraudulent identification. It is worth noting that many of those that assisted the hijackers did so without knowledge of their September 11, plans.

Effective measures will be difficult to achieve in any event. The integrity of any verification system—even a computer-based "paperless" one—hinges on the security of the documents which underlie it, and such "breeder" documents are not secure. The birth certificate is a "breeder" document in that it can be used to obtain an identity document such as a U.S. passport, driver's license, military I.D. or social security card.

However, if these issues are going to be examined, we want them to be examined in a balanced fashion. We need to decide just how far we are willing to go in dealing with this problem. For instance, birth and death records are certain to be used, and we need to examine just what resources we need to dedicated to revamping these record-keeping systems. We must deal with issues of efficiency and resources in a complimentary fashion as opposed to pitting these issues against one another. The same is true of revising SSA and INS databases. Are we willing to bear the costs of developing and maintaining such gigantic data bases?

However, if these issues are going to be examined, we want them to be examined in a fair and equitable way. The fight against counterfeit documents and fraud should not become a fight against personal privacy that leads to a national ID card. I do not want a national ID card to be demanded of Americans every time they engage in what should be routine activity that can be conducted anonymously and without government intervention.

Technology has played a vital role in advancing freedom around the world, but it also has laid new temptations at the doorstep of government. Once the technology

and a database are in place for a system such as a national worker registry, alternative uses for the registry will arise. This temptation can occur every time a new “national crisis” emerges: to help fight the war on drugs, to control the spread of disease, or to combat the War on Terrorism.

Congress also must take care to avoid steps that would increase rather than diminish immigration-related discrimination that has already become a feature of our employment system. In response to employer sanctions, many employers have screened out all “foreign-looking” or “accented” job applicants; have adopted illegal “citizens-only” hiring policies. They have selectively applied verification procedures only to “suspect” employees and demanded documents when hiring foreign-sounding employees when compared to other employees.

We also have to be mindful of states’ rights. We should not become so aggressive in this area that states are turned into mere tools of the federal government in connection with the identity documents they issue.

Finally, Mr. Chairman, I hope that we can work cooperatively, and in the true spirit of bipartisanship to eliminate identity fraud and theft and make the necessary changes in the law that must be made. However, I would like to say for the record that although there is ample and substantial evidence of the existence of identity fraud and theft, this hearing should in no way be used as a vehicle to discourage talented men and women from different countries from coming to the United States to study, to exchange creative thought and ideas, or to discourage businesses from temporarily moving their employees to contribute to our economy and our way of life. We should discourage identity theft and fraud, but not discourage fair and equal opportunity either. Thank-you Mr. Chairman.

Mr. GEKAS. Which brings to mind the general practice that we will accept the written statements of the witnesses for the purposes of inclusion in the record, and then accord each witness 5 minutes or so—mostly 5 minutes, less so—to review the contents of the written statement. We’ll begin with Mr. McNulty and the 5 minutes that will be the general rule.

**STATEMENT OF PAUL J. McNULTY, UNITED STATES  
ATTORNEY, EASTERN DISTRICT OF VIRGINIA**

Mr. McNULTY. Thank you very much, Mr. Chairman. I’m delighted to be back with you in this room. It holds so many memories for me; as you mentioned, 8 years I spent with this prestigious Committee. And this Committee actually in my time here formed an outstanding foundation for me as I now serve as U.S. Attorney in the Eastern District of Virginia, enforcing the laws that are drafted by this Committee, and understanding those laws is a very beneficial thing. So I am very happy to be back here now and seeing old friends again.

In the weeks before September 11, nearly a year ago today, Victor Lopez-Flores and Herbert Villalobos were sitting out front of the Dollar Store in Arlington, Virginia, across the street from the DMV, the Department of Motor Vehicles, Virginia. This is a place where they hung out a lot. The reason why they hung out there was because of the location of the DMV across the street. You see, Victor and Herbert were in the business of helping people acquire false, fraudulent, driver’s licenses or ID cards from the Department of Motor Vehicles.

Well, 1 day last August, as they were sitting in front of the Dollar Store, a van pulled up. It had out-of-State plates, New York, New Jersey—I can’t remember now exactly what they were—and three men got out of the van, three Middle Eastern men, and they approached Victor. They knew that they were coming to him for a particular reason. And they asked him to help them to do what Vic-

tor was there to do, and that is to acquire Virginia identification cards.

They talked to Victor and to Herbert for a little while, and they haggled over the price, and they agreed to pay \$100 per person for the identification card.

So Victor and Herbert said, Get back in your van and follow us. And Victor and Herbert drove off in their car, and they drove down the street to a notary and a law office. And Victor walked into this law office, and he knew exactly what he was doing, and he had been in there many times before. And he took these three people, these three individuals who he did not know, he took them to this notary, Ms. Galicia, and she handed them two forms. One was an identification document. The other was a residency certificate.

The men signed the identification document, and Ms. Galicia notarized it and got the signature of a lawyer there in the office.

Then she took the residency form, and she handed it to Victor and then another one to Herbert, and they signed that form, and it was notarized, and they indicated that they knew that these three gentlemen were Virginia residents. They certified that they were Virginia residents.

And then they got back in their cars and they drove back to the DMV, and with those two forms, that identification document and that residency certificate, they dropped them off in front of the DMV. The three men walked into the DMV. They were already instructed as to what to do when they got in there, but Victor and Herbert were in the business of taking many people into the DMV to show them how to make their way—their way through the lines and so forth and to fill out the application inside. Those three men went in and got Virginia identification documents.

A few weeks later, those three men were on Flight 77, and they were the alleged hijackers of that plane that flew into the Pentagon and killed 189 people, the worst violent crime in the history of Virginia, and part of the tragedy and attack of September 11.

So those three men were part of actually seven out of the 19 hijackers who acquired false Virginia identification cards. And they were one—there were many others who were accomplices or associates of one kind or another who have now been convicted in the Eastern District of Virginia, along with Victor Lopez Flores and Herbert Villalobos, and Ms. Galicia for this fraudulent ID scam.

Why was this so important? Well, we don't know for sure, but what we think was going on was that, in order to get the tickets at the counter, they needed to show proof of identity. And what better proof at Dulles International Airport than a Virginia identification card or a Virginia driver's license. That card was an essential tool in the process of committing those horrid crimes.

And this is a problem that we have seen in Virginia in an enormous—to an enormous extent. It is the equivalent, that is, acquiring this false identification, it's the equivalent to a criminal acquiring a gun. False or stolen IDs have become a tool of the trade.

We prosecuted a case involving the Virginia driver's licenses and identification cards that was a scheme that included tens of thousands of false Virginia identification cards and driver's licenses being provided, mostly to illegal immigrants. That case, the case of Jennie Wrenn, which was prosecuted in February of last year, was

a scheme involving drivers and middlemen that would pick individuals up all up and down the East Coast and for a fee of \$500 to \$1,000, bring them to Virginia and then come into Ms. Wrenn's operation, a real estate business, a front business, and pay a very small fee of \$45 for those same documents I just described in the case of the hijackers. And there were many other people in the same business as Ms. Wrenn, which led to, again, tens of thousands of false IDs being acquired in Virginia. That's the story of the Virginia driver's license in a nutshell.

We have also an extensive problem with the false Social Security numbers, and the extent of that fraud covers our airport problem and credit card fraud and so forth. And I know in the interest of time, I don't want to repeat my testimony, but let me just say with regard to the airport initiative, we looked at 28,000 people who had secured badges, that is, badges that gave them access to almost any spot in the airport. We looked at 28,000 people who had that security badge in five major airports in eastern Virginia. And of those individuals, we identified 75 who had used a false Social Security number to gain their security badge. Those Social Security numbers can either be a made-up number or a stolen number. And, again, taking a false Social Security number is the foundation for credit card theft and other crimes, all of which we've prosecuted in the district.

Am I—has my time expired? Thank you, Mr. Chairman. I'd be happy to talk in more detail about how we're addressing that in the Eastern District.

Mr. GEKAS. Yes, we'll give you an opportunity to amplify during the question and answer session.

[The prepared statement of Mr. McNulty follows:]

#### PREPARED STATEMENT OF PAUL J. McNULTY

Messrs. Chairmen and Members of the Subcommittees: As the United States Attorney for the Eastern District of Virginia, I am privileged to serve the public and to lead a talented staff in a district on the front lines of the war against terrorism. It is also my privilege to appear before you today to discuss the substantial problem of false and stolen identities. This is an extremely important topic, and I commend you for holding this hearing.

Attorney General Ashcroft and the Department of Justice consider identity theft to be a serious problem that requires national attention from our prosecutors. On May 2nd, the Attorney General announced a nationwide sweep of identity theft cases, in which 73 federal criminal prosecutions were brought against 135 individuals in 24 districts. In addition, to strengthen current federal identity theft legislation, the Attorney General announced that the Department would seek legislation to enhance criminal penalties in identity theft-related cases. S. 2541, introduced with bipartisan support, would not only establish a new provision for aggravated identity theft but would also expand the reach of the current statute.

In the nine months since I became the United States Attorney, I have seen how the problem of false and stolen identities permeates almost every aspect of federal law enforcement in the Eastern District of Virginia. We have prosecuted individuals who steal the identities of others or who create false identities to defraud banks, credit card companies, other businesses, and government agencies. Collectively, these people have caused hundreds of millions of dollars in losses and ruined the credit histories of hundreds of hard-working, honest Americans. Unfortunately, terrorists, criminals, and illegal aliens turn to Virginia with alarming frequency to establish a false or fictitious identity.

## FALSE OR FICTITIOUS VIRGINIA DRIVER'S LICENSES

Seven of the September 11th hijackers<sup>1</sup>—none of whom actually lived in the Commonwealth—had obtained Virginia driver's licenses by submitting false proof of Virginia residency.<sup>2</sup> One of the seven, Ziad Jarrah, was involved in the failed attempt to fly Flight 93 into a target here in the Washington, D.C., area; two were aboard the airplanes that crashed into the World Trade Center; and four were aboard Flight 77 when it was flown into the Pentagon.

Virginia has always required both proof of identity and proof of Virginia residency to obtain a Virginia driver's license. There is a long list of documents that can be used to establish identity and residency. The feature of the law that the terrorists exploited allowed them to establish Virginia residency by submitting a notarized affidavit of another Virginia resident. For example, two of the September 11th hijackers paid \$100 to an illegal immigrant—who had himself fraudulently obtained his Virginia driver's license—to execute the residency affidavit for the hijackers before a notary public. With this notarized affidavit, the hijackers had sufficient “proof” of Virginia residency to obtain Virginia driver's licenses. After the connection with the September 11 hijackers was discovered, the Virginia Department of Motor Vehicles moved quickly to change its procedures. As of September 21st, the notarized forms were taken off the list of acceptable documents, and the Virginia General Assembly has ratified that decision by amending the relevant state statute effective this July 1st.<sup>3</sup>

## TRAFFICKING IN FALSE OR FICTITIOUS IDENTITIES

Terrorists are not the only people using false and stolen identities to undermine our security and our economy. There is a substantial cottage industry of manufacturers and traffickers in false identity documents and stolen credit cards. You need not walk more than a few blocks from this hearing room to meet someone who will sell you a fake social security number for about \$80. If you go online, you may even be able to obtain Social Security numbers from various websites for little or no money. Stolen credit cards and even stolen identities may also be purchased for the right price. Once you have a false identity, or someone else's identity, and a credit card number tied to that false or stolen identity, you can wreak havoc—for a short time you can buy anything you want, travel wherever you want, and do almost anything you desire, knowing that you'll never have to pay, and that someone else will be stuck with the bill. Or, if your goals are more deadly and you have more patience, you can quietly build a life under your assumed identity in anticipation of a future terrorist act.

Our Office's prosecution of a Virginia notary public named Jennifer Wrenn illustrates how criminals traffic in false or fictitious Virginia driver's licenses. Ms. Wrenn owned and operated two offices in Falls Church and Manassas Park, Virginia, from which she ostensibly conducted the activities of her real estate business, Jenni Wrenn Realty. An investigation by the Virginia DMV, the INS, and the IRS revealed, however, that the true work at both offices was the sale of fraudulent forms<sup>4</sup> to immigrants seeking to obtain Virginia driver's licenses and identification

<sup>1</sup>The seven were Hani Hanjour, Khalid Almihdhar, Majed Moqed, Salem Alhazmi, Abdulaziz Alomari, Ahmed Alghamdi, and Ziad Jarrah. It is suspected, but not known, that these seven hijackers used their Virginia identification cards or licenses to board the flights they later hijacked.

<sup>2</sup>Since September 11, 2001, this Office has prosecuted four individuals who helped the hijackers complete fraudulent forms and submit them to the Virginia Department of Motor Vehicles (“DMV”). All four were charged with and pled guilty to identification document fraud, in violation of 18 U.S.C. § 1028. In addition, this Office has used 18 U.S.C. § 1028 to prosecute several people who came to our attention through the 9/11 investigation, either due to their contacts with the hijackers or because of their presence near Dulles airport on September 11th with flight manuals. We also prosecuted two men who ran a checkpoint at the Pentagon in a tow truck in February of this year. In each of these cases, the defendant submitted false information to the Virginia DMV to obtain a Virginia identification card or license for himself or another by fraud.

<sup>3</sup>This change is a step in the right direction and has had an impact. Nonetheless, I think it is too soon to tell if this change is sufficient to prevent the abuse of the system that occurred before September 11th. Prior to this change, many illegal immigrants and ineligible drivers from other states traveled to Virginia to obtain Virginia licenses and identification cards by fraud.

<sup>4</sup>In order to obtain a Virginia identification card or driver's license, an applicant must provide the DMV with proof of identity and Virginia residence. Only Virginia residents may obtain a Virginia driver's license or identification card. Prior to September 22, 2001, an applicant lacking documentary proof of identity and Virginia residence could submit sworn statements of identity and residence in lieu of documentary proof. In particular, an applicant lacking proof of identity could submit an identity affidavit (DMV Form DL6), and an applicant lacking proof of Virginia



cards. Immigrants were coming to Ms. Wrenn through a network of paid drivers and middlemen with whom Ms. Wrenn worked. For a fee of between \$500 and \$1,000, these drivers and middlemen would bring immigrants from New Jersey, Connecticut, New York, and other states throughout the country to Ms. Wrenn's offices. Once there, Ms. Wrenn and her staff would complete fraudulent forms for the immigrants for a fee of \$45. These fraudulent forms bore all the necessary signatures and affirmations, and falsely stated that the applicants were residents of Virginia. At the height of her business, Ms. Wrenn was providing fraudulent forms to over a thousand immigrants a month.

The Wrenn case demonstrates how pervasive this type of fraud can be. Jenni Wrenn was but one of several notaries or attorneys who were selling fraudulent forms to illegal aliens from other states. Indeed, prior to the attacks of September 11, 2001, thousands of illegal aliens from all over the United States were coming to Virginia each month to obtain fraudulent licenses or identification cards.

Ms. Wrenn was arrested in February 2001, and subsequently convicted at trial of seven counts of conspiracy, identification document fraud (18 U.S.C. § 1028), encouraging illegal immigration, and money laundering. In addition, the government arrested and prosecuted a dozen other individuals who worked with her or for her on charges of identification document fraud. These individuals included a lawyer, notaries, drivers, and other middlemen.

#### SOCIAL SECURITY NUMBER FRAUD

Our Office's prosecution of Ousmane Sow and Aboubakar Doumbia for social security fraud illustrates how easily social security cards are obtained by fraud and how widespread the abuse is. Sow and Doumbia were caught at Reagan National Airport in transit from New York to Miami. They were traveling on tickets paid for with stolen credit cards and were found to be carrying a dozen foreign passports and two dozen stolen immigration forms. Both men were charged with immigration fraud and pled guilty prior to trial. Interestingly, both had fraudulent Virginia identification cards even though they lived in New York.

One of the two men agreed to cooperate with the government and revealed the purpose of their trip to Miami. He informed investigators that he and his accomplice were part of a West African criminal syndicate (he used the term "crew") based in New York City. This syndicate specialized in the fraudulent procurement of social security cards and, to a lesser extent, the fraudulent procurement of Virginia driver's licenses and identification cards. According to the cooperating defendant, members of the syndicate repeatedly traveled from New York to major cities in the United States on tickets paid for with stolen credit cards. The purpose of the trips was to apply for social security cards by fraud at the Social Security Administration offices in each city. At each office, the members of the syndicate would apply for a card using a passport and an INS form.<sup>5</sup> The members of the syndicate altered the passports by substituting their own photographs so that they could apply in person for a social security card in the name of one of the syndicate's clients (to whom the passport actually belonged). They further placed doctored INS forms in the client's passport to make it appear that they, the applicants, were lawfully in the United States and had the right to work. In fact, their clients were illegal immigrants in New York and New Jersey who paid the syndicate between \$700 and \$1,500 for a social security card. According to the cooperating defendant, members of the syndicate had traveled to all of the major cities in the United States, often more than once, and obtained well over a thousand fraudulent social security cards.

The use of false or fictitious social security numbers appears to be widespread. Our office recently completed an airport security initiative that involved the review of over 28,000 workers at the major commercial airports within the Eastern District of Virginia.<sup>6</sup> The review revealed that seventy-five (75) airport workers used false or fictitious social security account numbers to obtain security badges<sup>7</sup> that afforded them unescorted access into the most sensitive areas of our airports. Many of these airport workers also used the same false or fictitious social security number to ob-

---

residence could submit a residency certification (DMV Form DL51). In theory, the identity affidavit had to be reviewed and signed by a Virginia lawyer, and the residency certification had to be signed by a Virginia resident who swore to the applicant's Virginia residence. In practice, both forms were subject to widespread fraud and abuse. Indeed, the forms were used primarily by illegal immigrants and ineligible drivers from other states to obtain Virginia licenses and identification cards by fraud.

<sup>5</sup>The form used was an INS form I-94, which is a record of authorized entry.

<sup>6</sup>Ronald Reagan Washington National (5,000), Dulles International (15,000), Richmond International (4,862), Norfolk International (3,386) and Newport News/Williamsburg (199).

<sup>7</sup>The badges are security identification display area or "SIDA" badges.

tain Virginia driver's licenses, fill out immigration forms, or apply for credit cards. Without a fraudulent social security number, none of the 75 airport employees could have obtained a security badge.

#### FALSE SOCIAL SECURITY NUMBER USED WITH A FALSE OR STOLEN IDENTITY

Criminals will also use both a false social security number and a false or stolen identity. For example, Rahila Aamir and Malik Raza, who were recently convicted of mortgage fraud in the Eastern District of Virginia, submitted loan applications to mortgage lenders under a false social security number and under the false name of "Mohammed Nasir" to gain approval for two loans, each worth approximately \$200,000. There is, however, no evidence that the Mohammad Nasir who signed the loan documents exists. The defendants obtained the false social security number by stealing it from an individual who lives in another part of the country. The defendants also appropriated the employer identification numbers of local businesses to fill out false W-2 forms that they used to prove to the lender what turned out to be nonexistent income. When the defendants defaulted on their loans, the lenders were not able to hold the defendants accountable for the losses since the defendants used false identification to obtain their loans.

#### FALSE IDENTITIES IN "BUST OUT" SCHEMES

We have also seen the use of false identities in so-called "bust-out" schemes. In these schemes, the criminals use credit card terminals obtained by a shell or "front" business to apply charges to fraudulently obtained credit card numbers or accounts opened in false names or the names of innocent victims. The criminals run the cards or numbers through the terminals but do not provide any goods or services. The credit card company credits the account of the front business because they do not know that the goods and services have not been provided to the card holder<sup>8</sup> or that the card holder is not a real person. Before the transaction can be reversed, the funds are moved out of the front business's account.

It is important to note that the credit card "bust out" scheme involves defendants who have stolen social security numbers to create false identities. Using these false identities, the defendants obtain credit cards which they use to commit the bust-out schemes, as described above. Once they bust out a card, they obtain another social security number and false credit card, and start the whole process over.

#### IDENTITY THEFT

In January of this year, I created one of the largest cybercrime units in the country dedicated to combating electronic crimes such as identity theft. Additionally, our Office has prosecuted several individuals for stealing the identifying information of others and using it to commit fraud. In several cases, the defendants stole individuals' checks and other information, including bank statements, from their mailboxes. For example, our Office prosecuted Edwin Ijaseun, who counterfeited stolen checks and used the individuals' addresses, dates of birth, and Social Security numbers obtained from the stolen documents to create false driver's licenses in the victims' names, but with the defendants' photographs. The false driver's licenses enabled the defendants to take the counterfeit checks to various branches of the account holders' banks and to successfully cash the checks.

In other cases, the defendants stole identifying information from the places where they worked. For example, our Office prosecuted Robert Magnuson, who had a temporary job that gave him access to the computer system containing the other employees' personal information. He used that information to apply for many credit cards. Once he obtained the credit cards, he then used the cards to withdraw cash from ATM machines. We have been investigating other individuals who have similarly obtained credit cards using stolen identities and used the cards to make purchases over the Internet. Frequently, these defendants have the merchandise shipped to commercial mailboxes opened in the names of the individuals whose identity they have stolen.

In most of these cases, the banks and the merchants have usually suffered the ultimate financial losses. The victims who had their identities stolen, however, have had to work for days, weeks, and sometimes months to obtain reversals of the charges, change their accounts, and restore their credit histories.

<sup>8</sup> Card holders who participate in bust-out schemes normally refuse to pay the credit card companies for the bogus purchases. Oftentimes, the card holders will file for bankruptcy to absolve themselves from having to pay their accumulated debt. On their bankruptcy applications, the card holders typically make false statements by lying about the reasons for accumulating such debt, and/or even their true identities.

## CONCLUSION

In prior generations, identity theft was not the problem that it is today. Simply put, people in the community knew each other. And if you were not well known in the community—or if you were known by your neighbors not to pay your debts—you had to use cash. If you were unfortunate enough to be in a strange town without money, you had to hope for a wire transfer from somewhere like Western Union. Not so today. We can go anywhere and buy anything, paying by credit, check, or debit. Like the well known credit card commercial used to say: “It’s everywhere you want to be.”

It is essential in today’s world that we know that people are who they say they are. Airport officials need to know that travelers are who they say they are. An employer needs to know that an applicant is who she says she is. From buying groceries to purchasing a firearm, merchants must know that a customer is who he says he is. Our whole system depends upon people being who they say they are. False or stolen identities undermine our whole system of commerce as well as our national security.

Mr. Chairmen, thank you for the opportunity to address this hearing on these important issues. I would be pleased to answer any questions you might have.

Mr. GEKAS. We turn to Mr. Huse.

**STATEMENT OF JAMES G. HUSE, JR., INSPECTOR GENERAL,  
SOCIAL SECURITY ADMINISTRATION**

Mr. HUSE. Good afternoon, Chairman Gekas, Chairman Smith, Ms. Jackson Lee, Mr. Scott. Let me first thank you for the invitation to be here today. This is a vitally important matter and a complex one, but I will begin my testimony with a simple declarative sentence: The Social Security number is our national identifier. Nine months ago, that statement was challenged by many. Today, it is an accepted fact.

Today’s hearing focuses on the integrity of the Social Security number with respect to those who arrive at our borders as visitors. You should be aware that this is only one portion, albeit a critical one, of our efforts to protect the SSN’s integrity.

In calendar year 2000, the Social Security Administration issued approximately 1.2 million SSNs to non-citizens, but issued over 5.5 million SSNs in all—5.5 million. While SSNs issued to non-citizens thus represent only about 20 percent of the total, the volume is significant and the implications, as we have learned, are serious.

While the Office of Inspector General is unable at this time to state unequivocally that any of the September 11 terrorists were enumerated by SSA itself, the investigation into the events of that day and the homeland security efforts aimed at preventing future attacks have revealed the importance of the SSN to any attempt at assimilation into American society.

It is now clear that the SSN is our national identifier, and protecting the integrity of that identifier is as important to our homeland security as any Border Patrol or airport screening.

We have issued several audit reports over the past 3 years, each identifying weaknesses in the enumeration process, the process by which SSA issues SSNs. The most important of these vulnerabilities was SSA’s procedures for verifying documents submitted with SSN applications. We have recommended on several occasions that SSA verify with the Immigration and Naturalization Service the authenticity of immigration documents submitted by non-citizens seeking to obtain an SSN.

Although there was a time that SSA opposed that recommendation, this is certainly no longer the case. Commissioner Barnhart

recognizes how critical it is to keep SSNs out of the hands of those who may seek to harm us and efforts to provide for INS authentication of immigration documents are accelerating. So, too, are plans for the Enumeration at Entry Program by which non-citizens entitled to SSNs will be processed at the time of their entry into the United States.

In the interim, the Commissioner announced earlier this year that SSA would no longer issue SSNs to non-citizens solely for the purpose of obtaining driver's licenses. And, more recently, she has announced that, beginning July 1st in selected cities and this fall nationwide, SSA will cease the issuance of SSNs to non-citizens if their immigration records have not been verified with the INS.

This will likely result in delays that would previously have been thought unacceptable by SSA, but I applaud the Commissioner's courage in making this stand.

Preliminary results of a study prepared by my office suggests that as many as 100,000 of the 1.2 million original SSNs issued to non-citizens during calendar year 2000 were based on invalid immigration documents that went undetected by SSA. We believe, and Commissioner Barnhart agrees, that this 8-percent error rate is unacceptable and that more must be done.

If the Federal Government is to meet its responsibility with respect to the SSN's role in the homeland security rubric, it will require the same type of interagency cooperation that President Bush spoke of in his address to the Nation several weeks ago. Besides the needed cooperation of SSA and the INS, it will also require the coordinated interactivity of Federal, State, and local government agencies, each ensuring the authenticity of the identification documentation presented to apply for an SSN.

The operations in which our office has participated in some 18 airports across the country over the past several months are but one way in which these efforts continue. Working with joint terrorism task forces and other Federal agencies under the aegis of Offices of the United States Attorney, we have worked to ensure that no airport employee who has misrepresented his or her SSN and identity has access to secure areas of the Nation's airports. A total of 432 people have been arrested to date and, more importantly, have been denied access to the areas which represent a significant terrorism vulnerability. Similar operations are in the planning stages at other sensitive facilities around the country.

We appreciate your interest in these issues and look forward to working with you to enhance the safety of all Americans. Thank you, and I'll be happy to answer any questions.

[The prepared statement of Mr. Huse follows:]

PREPARED STATEMENT OF JAMES G. HUSE, JR.

#### INTRODUCTION

Good afternoon, Chairman Gekas, Chairman Smith, Ms. Jackson Lee, Mr. Scott. Let me first thank you for the invitation to be here today. This is a vitally important matter, and a complex one, but I will begin my testimony with a simple, declarative sentence: The Social Security number (SSN) is our national identifier. Nine months ago, that statement was challenged by many. Today, it is an accepted fact.

Today's hearing focuses on the integrity of the SSN with respect to those who arrive at our borders as visitors. You should be aware that this is only one portion—albeit a critical one—of our efforts to protect the SSN's integrity. In calendar year

2000, the Social Security Administration (SSA) issued approximately 1.2 million SSNs to non-citizens, but issued over 5.5 million SSNs in all. While SSNs issued to non-citizens thus represent only about 20 percent of the total, the volume is significant.

#### MAINTAINING SSN INTEGRITY AT OUR BORDERS

We may never know with absolute certainty how many of the 19 hijackers of September 11th used improperly obtained SSNs, or how they obtained them. Following the September 11th attacks, the Office of the Inspector General (OIG) immediately received from the Federal Bureau of Investigation (FBI) the names and other personal identifiers (as they then knew them) of the 19 terrorist hijackers who died in these attacks. Those names and identifiers were matched against SSA's indices. We associated SSNs with 12 of the 19 names. Of the SSNs associated with these 12 names, 5 appeared to be counterfeit (SSNs that were never issued by SSA). In addition, 1 was associated with a child, leaving 6 names associated with SSNs that were issued by SSA. Further, 4 of these 6 names were associated with multiple SSNs. At this juncture, we cannot assert whether any of the 6 subject names associated with these SSNs are, in fact, September 11th terrorists.

It is important to understand that our investigative efforts may ultimately determine that certain of these six individuals possessed legitimate (or well-crafted counterfeit) documents to legitimately obtain an SSN. These documents may then have been cleared for entry to the United States by the vetting processes of both the Department of State, and the Department of Justice's (DOJ) Immigration and Naturalization Service (INS), thereby facilitating the assignment of an SSN under the procedures in place at that time. In view of this, and other imperatives following the terrorist incidents, the SSA established an Enumeration Working Group to develop and recommend to the Commissioner, both internal and external process changes that will result in strengthening the integrity of the issuance of SSNs. Many of these changes have been made and others are pending implementation in the near term. My office has been a committed partner with SSA in all the activities of that workgroup.

Regardless of what is eventually proven or disproven, the investigation into the events of that day, and the homeland security efforts aimed at preventing future attacks, have revealed the importance of the SSN to any attempt at assimilation into American society. Nine months later, no one harbors any illusion that the SSN remains simply a number for the tracking of workers' earnings and the payment of social insurance benefits. The SSN is our national identifier, and protecting the integrity of that identifier is as important to our homeland security as any border patrol or airport screening.

We have long been aware that failure to protect the integrity of the SSN has enormous financial consequences for the government, the people, and the business community. We now know that the burden that the enumeration process carries can have far graver consequences than previously imagined and as such, SSA can no longer afford to operate from a "business as usual" perspective. Whatever the cost, whatever the sacrifice, we must protect the number that has become our national identifier; the number that is the key to social, legal, and financial assimilation in this country.

We recognize that SSA alone cannot resolve the monumental issues surrounding homeland security. Efforts to make our Nation safer will involve new or expanded initiatives by almost every segment of our population, including State and local governments, private industry, non-governmental organizations, and citizens. However, we also recognize that, in endeavoring to protect our homeland, no government system or policy should be ignored. As such, SSA, as a Federal agency and public steward, must continue its efforts to strengthen its systems and processes to minimize the use of SSNs for illegal purposes. We believe that SSN integrity is a link in our homeland security that must be strengthened and sustained.

Last month, we issued a Management Advisory Report entitled *Social Security Number Integrity: An Important Link in Homeland Security*. In that report, we stated that it is critical that SSA independently verify the authenticity of the birth records, immigration records, and other identification documents presented by an applicant for an SSN.

This is a relatively new issue for the American people, but it is an old issue for us. Two years ago, in May 1999, we issued another Management Advisory Report entitled *Using Social Security Numbers to Commit Fraud* (A-08-99-42002), in which we described significant vulnerabilities in SSA's enumeration process. The most important of these vulnerabilities was SSA's procedures for verifying documents submitted with SSN applications. In September 2000, we issued yet another

report, *Procedures for Verifying Evidentiary Documents Submitted with Original Social Security Number Applications*, in which we identified similar weaknesses. While each of these reports dealt with across-the-board weaknesses, rather than weaknesses associated only with enumeration of non-citizens, each report did address the non-citizen issue at length.

In both of these reports, as in last month's report, we recommended that SSA independently verify birth and immigration records submitted in support of SSN applications. Additionally, we recommended full and expedited implementation of a joint Enumeration at Entry program in which the Agency would issue SSNs to non-citizens upon their entry into the United States based on information obtained from INS and the Department of State.

At the time the 1999 and 2000 reports were issued, SSA disagreed with our recommendation to independently verify birth and immigration records. The Agency stated that delaying the receipt of SSNs for thousands of non-citizens, most of whom were legitimately entitled to a number, was not acceptable. Rather, they preferred to work with the INS on improving existing systems until the recommended Enumeration at Entry program could be implemented.

Unfortunately, until September 11th, SSA had limited success encouraging the INS to move quickly on either of these planned initiatives, as the projects did not appear to be as high a priority to INS as they were to SSA. For example, in August 1999, SSA's Commissioner wrote to the Commissioner of INS regarding SSA's concerns with the current verification process and SSA's hope that the two Agencies could expeditiously move to implement the Enumeration at Entry program. Although some staff-level meetings continued between representatives of the two agencies, SSA never received a formal response to the letter. As such, SSA requested assistance from the Office of Management and Budget (OMB) to move the initiatives along. In response, OMB convened a meeting between the two agencies. Still 2 years after that, little progress was made, although SSA does report that in the months since September 11th, negotiations with INS are proceeding more smoothly and at a faster pace.

Commissioner Barnhart has indicated her intention to begin holding non-citizens' applications for new SSNs until their evidentiary documents can be verified with the INS. I applaud her decision, and her resolve. While SSA is justifiably proud of its reputation for timely service, Commissioner Barnhart's decision to refine this commitment to include a balance for both enumeration integrity and the security of our Nation's borders is a sound one.

Our own work illustrates just how wise a decision this is. In a recent study, preliminary results indicate that 8 percent (over 100,000) of the 1.2 million SSNs assigned to non-citizens during Calendar Year 2000 were based on invalid immigration documents, which current SSA processes did not detect. We have no way of determining how many SSNs have been improperly assigned to non-citizens throughout history. However, we believe—as does Commissioner Barnhart—that in the interest of homeland security, an 8 percent error rate, 1 out of every 12 SSN cards, is unacceptable and further action is required.

The following examples from our study are representative of how non-citizens improperly obtained SSNs by presenting invalid documents:

- SSA assigned SSNs to two individuals (both age 28) purporting to have been born in India. These individuals provided immigration documents improperly showing them as work-authorized; however, INS had no record of the two individuals.
- SSA assigned an SSN to a 27-year-old male purporting to have been born in Japan. He presented a work-authorized immigration document to SSA, although INS never authorized him to work. Specifically, he presented an INS document indicating he was an intra-company transferee and, therefore, eligible for a work-authorized SSN. However, INS reported to us that he was actually the spouse of an intra-company transferee and, therefore, he was not eligible for a work-authorized SSN.
- SSA assigned an SSN to a 56-year-old female purporting to have been born in Mexico. She presented a work-authorized document. However, INS had not authorized her to remain in the country. She originally entered the country with an "H2-B" classification (temporary worker performing services of labor unavailable in the United States). She applied for an SSN on December 20, 2000, with INS documents indicating her H2-B status. Therefore, SSA assigned the individual an SSN. Nevertheless, INS confirmed that her authorization to remain in the United States expired December 1, 2000, and INS found no indication that she applied for an extension. Accordingly, the docu-

ment she presented to the SSA field office when applying for an SSN was already invalid.

These examples appear relatively harmless, but they demonstrate the ease with which any immigrant can fool well-intentioned SSA employees into issuing a critical identity document.

#### SSNS, IMMIGRANTS, EMPLOYERS, AND THE EARNINGS SUSPENSE FILE

One of the first steps in obtaining employment and realizing the goals of many U.S. immigrants is obtaining an SSN. Most immigrants—about 75 percent—come to the United States legally, many to join close family members. However, INS estimated the undocumented immigrant population reached about 5 million in 1996, not including the 3 million who were given amnesty under the Immigration Reform and Control Act of 1986. Additionally, the INS estimates the number of undocumented immigrants continues to grow by about 275,000 individuals each year.

To improperly acquire an SSN, undocumented immigrants may either apply for a “legitimate” SSN using false evidentiary documents (as in the examples given above, or by using counterfeit passports or other falsified foreign documents) or they may create or purchase a counterfeit Social Security card. Additionally, if an undocumented immigrant is not required to show a Social Security card (which is very often the case), he or she may simply invent a nine-digit number. This SSN may be one the Agency has already assigned to another individual (stolen SSN) or one never assigned (fake SSN).

SSA statistics show three industries (agriculture, food and beverage, and services) account for almost one-half of all wage items in SSA’s Earnings Suspense File (ESF). The ESF is the Agency’s record of annual wage reports submitted by employers for which employee names and SSNs fail to match SSA’s records. Of these industries, agriculture is the largest contributor, representing about 17 percent of all ESF items. In fact, in one study of 20 agriculture employers, we determined that 6 of every 10 wage reports submitted by these employers had incorrect names or SSNs. From 1996 through 1998, these 20 employers submitted over 150,000 wage items for which the employee’s name and/or SSN did not match SSA records, representing almost \$250 million in suspended wages over the 3-year period.

Because SSA has no legal authority to levy fines and penalties against employers or employees who submit incorrect SSN information on wage reports, the Agency relies upon other Federal agencies to assist in combating SSN misuse. Specifically, as provided by law, SSA must rely on the Internal Revenue Service (IRS) to enforce penalties for inaccurate wage reporting and upon the INS to enforce immigration laws. Unfortunately, the IRS has been reluctant to apply penalties and SSA and the INS have had limited collaboration on the issue.

We believe applying penalties would have a ripple effect on employers who consistently submit wage reports for employees whose names and SSNs do not match SSA’s records. Although SSA is primarily interested in penalizing the most egregious employers, IRS staff expressed concern with the application of even these penalties. IRS senior staff members believe they and SSA would have a difficult time determining whether an employer exercised appropriate diligence in obtaining the necessary information from employees. SSA representatives, however, believe they could provide the IRS with sufficient evidence to show an employer knew or should have known its employees’ SSNs were incorrect.

Despite the IRS’ concerns, the two Agencies held discussions to explore the enforcement of an existing penalty provision (\$50 per incorrect wage report) for employers who repeatedly submit erroneous name and/or SSN information. To implement the penalty, SSA and the IRS agreed they must (1) jointly define the circumstances for applying penalties; (2) identify information needed from SSA for the IRS to support applying penalties; and (3) develop the proposed data flow and procedures to be followed.

In Calendar Year 2000, based on this agreement, SSA provided a list of 100 of the most egregious employers to the IRS. These employers represented the employers with the largest number of name/SSN match failures in consecutive years. The IRS expressed interest in the listing but, to date, has not assessed penalties.

Success of SSA’s coordination with the INS regarding non-citizens’ misuse of SSNs to obtain employment has also been minimal. In a previous audit report, we recommended that SSA (1) collaborate with INS on this issue and (2) reevaluate its application of existing disclosure laws or seek legislative authority to remove barriers that would allow SSA to share with the INS information regarding employers who chronically submitted incorrect wage reports. SSA disagreed with our recommendations and stated that its interpretation of the privacy and disclosure issues

is accurately applied and continues to provide appropriate disclosure guidance within existing authority.

The intent of our recommendations was to suggest that the Agency look for avenues under current law and regulations first before seeking legislative authority. We acknowledge SSA's efforts to combat SSN misuse and reduce the ESF's growth. However, given the magnitude of SSN misuse by unauthorized non-citizens, we continue to believe SSA should take preemptive and preventive measures to ensure the SSN's integrity. We continue to believe that the sharing of such information in certain situations would stem the growth of SSN misuse for employment purposes.

#### *Non-work SSNs*

SSA assigns "non-work" SSNs for limited purposes to non-citizens who do not have authorization from INS to work while they are in the United States. As of August 1997, SSA had issued approximately 7 million non-work SSNs. Since that time, the Agency has reduced the number of circumstances for which it will issue non-work SSNs. Although SSA has issued another 360,000 non-work SSNs since 1997, the number has been steadily declining in almost every year. For example, the number of non-work numbers issued dropped from approximately 128,000 in 1998 to 70,000 in 2001. Additionally, in March 2002, SSA notified the Nation's governors that it would no longer issue non-work SSNs for the purpose of getting a driver's license. As a result, the number of non-work SSNs issued in 2002 may be lower than 30,000.

We applaud SSA's efforts to minimize the number of non-work SSNs it assigns. Our audit work indicates that, despite the "not valid for employment" terminology that appears on every non-work SSN card, individuals frequently use these SSNs for just that purpose. For example, in Tax Year 2000, approximately 600,000 individuals with non-work SSNs used the numbers to work, earning over \$21 billion. Because SSA does not routinely learn of changes in a person's work authorization, not all earnings reported under a non-work SSN are attributable to non-authorized work. Under current guidelines, SSA will pay Old-Age, Survivors and Disability Insurance benefits based on the earnings obtained under non-work SSNs, as long as the number holders meet all benefit eligibility requirements. We disagree with this practice and have recommended that SSA seek legislation allowing the Agency to deny benefits to individuals who use non-work SSNs for employment purposes. SSA has elected not to seek such legislation.

#### *Suspended Wages and Notification of the Public*

SSA annually sends out between 7 and 8 million letters to employees and employers regarding the submission of wages where the SSN and associated name cannot be matched to SSA's records. Although these submissions may relate to the misuse of an assigned SSN, SSA does not notify the actual SSN holder. However, providing timely notifications may be difficult due to internal attempts to resolve the problems, while notifying the public may create unnecessary alarm.

The very fact that a reported wage item is in the ESF means SSA does not know the correct identity of the worker. For example, SSA has noted that about 55 percent of the items in the ESF have (1) no name, (2) no name and no SSN, or (3) an unissued SSN. The remainder of the items in the ESF generally relates to a mismatch between the name and SSN. Under a policy of notifying people whose SSNs are being falsely used, SSA could only take action on the missing or unissued SSNs since no specific member of the public is impacted by these wage items. However, the remaining wage items with a name and SSN mismatch would require further review by SSA.

SSA has a number of ongoing processes to obtain the correct name and SSN associated with the wages, such as correspondence with employees and employers, as well as manual and automated edits. These processes can take at least a year to complete, and often longer. However, through these processes, SSA is able to reinstate many of these wage items to the rightful owners' earnings records when, at first glance, it could have appeared to be the misuse of another individual's SSN. Sending a notice to the real owner of the SSN prior to these processes may be premature and unduly alarm the public.

Finally, both OIG and SSA reviews of the suspended wages in the ESF and the associated industries lead us to believe that illegal work, rather than identity theft, may be the primary cause of suspended wages. Many of the items in the ESF related to the agricultural industry, which hires transient employees who may or may not have work authorizations from the INS. These workers may create an SSN for the sole purpose of obtaining employment. In such cases, while these workers are providing fraudulent information to their employer, notifying the real owner of the



SSN that their number is being falsely used may create the impression of identity theft when in fact, the number was randomly chosen for the purpose of employment.

#### *Investigative Efforts*

Improving the integrity of the enumeration process is critical, but of course, it is prospective relief. Millions of SSNs have already been issued to non-citizens, many of them based upon fraudulent documentation, and more will be issued while SSA and the INS continue seeking improvements. Therefore, we continue our efforts on the investigative side to ensure that where the improper acquisition of an SSN by a non-citizen creates a possible homeland security risk, we are doing all we can to intervene.

The operations in which our office has participated in some 18 airports across the country over the past several months are but one way in which these efforts continue. Working with Joint Terrorism Task Forces and other Federal agencies under the aegis of Offices of United States Attorney, we have worked to ensure that no airport employee who has misrepresented his or her SSN and identity has access to secure areas of the Nation's airports. A total of 432 people have been arrested to date, and more importantly, have been denied access to the areas, which represent a significant terrorism vulnerability. Similar operations are in the planning stages at other sensitive facilities around the country.

As it became apparent in the aftermath of September 11th that the SSN would be an important element in the investigation of the attacks, our office worked not only with other investigative entities, but with DOJ to educate prosecutors on the acquisition, use, and misuse of SSNs by potential terrorists. A memorandum was distributed to United States Attorneys nationwide, explaining the use of 42 U.S.C. § 408(b)(7), Misuse of an SSN, as a charge that could be used to indict, arrest, detain, and where appropriate, deport suspected associates of the hijackers or others with links to terrorism. Because a terrorist, to be effective, must first be assimilated into American society, and because an SSN is a critical tool in the assimilation, it became apparent that the acquisition of an SSN was indispensable.

Lofti Raissi, for example, was long thought to be an associate of some of the September 11th hijackers, having trained with some of them at flight school in Arizona. When he was being held in London, investigation revealed that while in the U.S., he had been using the SSN of a deceased New Jersey woman.

Malek Seif, a licensed pilot and native of Djibouti, was living in Arizona until August 2001, when he left the U.S., only to surface in France, where he was detained by French anti-terror authorities. He was released in order to return to the U.S., where he was arrested upon his arrival at Phoenix Sky Harbor airport and charged with obtaining one SSN and one replacement Social Security card based on the presentation of false information to the Commissioner of Social Security, and a second SSN under a second identity on the basis of fraudulently obtained immigration documents. He pleaded guilty to multiple counts, including misuse of an SSN, in Federal court in Phoenix.

Sofiane Lamaiche, another suspected associate of some of the September 11th terrorists, and a one-time roommate of Lofti Raissi, was smuggled into the United States on an Algerian ship through the port of Philadelphia, and within five days, made his way to Phoenix and purchased a new identity, including an SSN. He was tried by an OIG attorney working as a Special Assistant U.S. Attorney in Arizona and convicted of multiple counts, including misuse of an SSN.

Finally, Redouane Dahmani, another suspected associate smuggled into the U.S., purchased a new identity, including an SSN. He then filed a false asylum application under his own identity (using Raissi as an affiant and interpreter), using the INS documents that resulted to obtain a "legitimate" SSN from SSA. He was charged at the Federal and State levels and is awaiting trial.

As the efforts of Federal law enforcement agents and prosecutors continue into the investigation of September 11th and the homeland security agenda, it becomes more and more apparent that those connected with terrorism will at some point obtain an SSN. They may buy it, they may create it, or they may obtain it from SSA directly through the use of falsified immigration records. But to operate in the United States, they need the number, and no additional time can be lost in taking those steps necessary to ensure that those numbers do not come from SSA.

#### CONCLUSION

In addition to large-scale operations such as those at the Nation's airports, and individual cases of those suspected of an association with terrorism, our efforts continue in other areas. We continue to meet with other Federal officials to ensure that we are doing all that restrictive privacy laws permit to assist DOJ and others to use SSN information in the homeland security context. We are in constant contact

with this and other committees of both houses of Congress to provide expertise and assistance in the analysis of data and creation of legislation aimed at protecting the SSN and preventing it from being used improperly. We have attorneys either working *as* Federal prosecutors or with them to enforce the Social Security Act's felony provisions. We continue our audit work, reviewing SSA's enumeration process and making recommendations for much-needed improvements. And we stand ready to do more. We appreciate your interest in these issues, and look forward to working with you to enhance the safety of all Americans.

Mr. GEKAS. We thank you, Mr. Huse, and we turn to the next witness. Mr. Stana?

**STATEMENT OF RICHARD M. STANA, DIRECTOR, ADMINISTRATION OF JUSTICE ISSUES, UNITED STATES GENERAL ACCOUNTING OFFICE**

Mr. STANA. Thank you, Chairman Gekas, Chairman Smith, Ms. Jackson Lee, Mr. Scott, and Members of the Subcommittees. I'm pleased to be here today to discuss the prevalence of identity fraud and its links to aliens' illegal activities. Generally, identity fraud encompasses a broad range of illegal activities based on fraudulent use of identifying information of a real person or a fictitious person. A pervasive type of identity fraud is identity theft, which involves stealing personal identifying information from someone like you or me, such as a Social Security number, a date of birth, or a mother's maiden name, and then using the information to create false identity documents, to fraudulently establish credit and run up debt, or to take over existing financial accounts. Other types of identity fraud involve fraudulent documents used by aliens to enter the country or illegally obtain employment and other benefits, and in some cases to facilitate a range of criminal activities, including terrorism.

My prepared statement discusses these and other topics. In my oral statement, I'd like to briefly make three main points.

First, although identity theft numbers are not easily captured and sometimes reflect different assumptions, the statistics we compiled show that the prevalence and cost of identity theft continue to rise and that the probability of getting caught remains low. Data from the three national credit bureaus, the FTC's identity theft data clearinghouse, and the Social Security Administration's IG fraud hotline show that the number of people reporting actual or suspected identity theft is increasing dramatically. Recent statistics on investigations and arrests by leading law enforcement agencies—the Secret Service, the SSA IG, the IRS, the FBI, and the Postal Inspection Service—also show an increasing trend in criminal activity. Further, the cost to the financial services industry in terms of documented bank fraud and payment card fraud exceeds \$1.8 billion from domestic operations alone.

Since 1998, the Congress and most States have enacted laws that criminalize identity theft. The passage of Federal and State identity theft legislation indicates that this type of crime has been widely recognized as a serious problem across the Nation.

My second point is that the use of fraudulent documents by aliens is extensive. With nearly 200 countries using unique passports, official stamps, seals, and visas, the potential for immigration document fraud is great. In addition, more than 8,000 State or local offices issue birth certificates, driver's licenses, and other

documents aliens can use to establish residency or identity. INS inspectors frequently encounter aliens who present fraudulent identity and/or various authorization documents in order to attempt illegal entry into the United States.

About half of the over 114,000 documents intercepted by INS inspectors last year were border crossing cards and alien registration cards, commonly called "green cards." Moreover, significant numbers of aliens unauthorized to work in the United States have used fraudulent documents to circumvent the employment verification process. Most of the fraudulent documents used were INS documents and Social Security cards. Some aliens have attempted to use fraudulent documents to illegally obtain other immigration benefits, such as naturalization or adjustment of status.

My third point is that identity theft or use of fraudulent documents often is an essential component of criminal activities, ranging from bank and credit card fraud to drug trafficking and international terrorism. For instance, INS has reported that although most aliens are smuggled into the country to pursue employment opportunities, some are smuggled as a part of criminal or terrorist enterprises. INS believes that as border enforcement activities increase, organized crime groups will increasingly use smugglers and fraudulent documents to facilitate illegal entry of individuals to engage in criminal activities.

The events of September 11 have underscored the urgency of effectively authenticating the identity of individuals. Terrorists have used and have been in possession of numerous false identification documents. For instance, conspirators involved in the 1993 World Trade Center bombing and the 1999 attempted LAX bombing were in possession of false identification documents. Terrorists' financing methods have been known to use various cash-smuggling and bank fraud activities that have been aided by identity theft.

Such instances raise other security questions related to identity fraud. For example, when an alien's identity documents are checked against a watch list at the border, can we be sure the individual is who he presents himself to be? When an individual presents identity documents for employment in sensitive occupations or areas, can we be sure the individual is who he presents himself to be?

Let me close by saying that most instances of aliens' using fraudulent identity documents appear to be related to entering the country and obtaining employment or other benefits. However, recent events dramatically illustrate that law enforcement officials need to be increasingly vigilant to other security vulnerabilities presented by identity fraud.

This concludes my oral statement. I'd be happy to address any questions the Members of the Subcommittee may have.

[The prepared statement of Mr. Stana follows:]

PREPARED STATEMENT OF RICHARD M. STANA

GAO	<hr/> <p>United States General Accounting Office</p> <hr/> <p>Before the Subcommittee on Crime, Terrorism and Homeland Security and the Subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, House of Representatives</p> <hr/>
-----	--

For Release on Delivery  
Expected at 4:00 p.m.  
Tuesday, June 25, 2002

## IDENTITY FRAUD

### Prevalence and Links to Alien Illegal Activities

Statement of Richard M. Stana  
Director, Justice Issues



---

Chairman Smith, Chairman Gekas, and Members of the Subcommittees:

I am pleased to be here today to discuss the significance of “identity fraud”—a term that encompasses a broad range of illegal activities based on fraudulent use of identifying information of a real person or of a fictitious person. A pervasive type of identity fraud is identity theft, which involves “stealing” another person’s personal identifying information—such as Social Security number (SSN), date of birth, and mother’s maiden name—and then using the information to fraudulently establish credit, run up debt, take over existing financial accounts, or to undertake other activities in another’s name. Also, another pervasive category is the use of fraudulent identity documents by aliens to enter the United States illegally to obtain employment and other benefits. The events of September 11, 2001, have heightened concerns about the contributory role that identity fraud plays in facilitating terrorism and other serious crimes.

In this statement, I make the following points:

- The prevalence of identity theft appears to be growing. Moreover, identity theft is not typically a stand-alone crime; rather, identity theft is usually a component of one or more white-collar or financial crimes, such as bank fraud, credit card or access device fraud, or the use of counterfeit financial instruments. Since 1998, the Congress and most states have enacted laws that criminalize identity theft. The passage of federal and state identity theft legislation indicates that this type of crime has been widely recognized as a serious problem across the nation.
- According to Immigration and Naturalization Service (INS) officials, the use of fraudulent documents by aliens is extensive. At ports of entry, INS inspectors have intercepted tens of thousands of fraudulent documents in each of the last few years. These documents were presented by aliens attempting to enter the United States to seek employment or obtain other immigration benefits, such as naturalization or permanent residency status. The types of false documents most frequently intercepted by INS inspectors include border crossing cards, alien registration cards, nonimmigrant visas, and passports and citizenship documents (both U.S. and foreign). Also, INS has reported that large-scale counterfeiting has made fraudulent employment eligibility documents (e.g., Social Security cards) widely available.

- 
- Federal investigations have shown that some aliens use fraudulent documents in connection with more serious illegal activities, such as narcotics trafficking and terrorism. This is a cause for greater concern.
  - Efforts to combat identity fraud in its many forms likely will command continued attention from policymakers and law enforcement. Such efforts will include investigating and prosecuting perpetrators, as well as focusing on prevention measures to make key identification documents and information less susceptible to being counterfeited or otherwise used fraudulently.

My testimony today will be based primarily on the results of work that we have completed in recent years, namely our May 1998 and March 2002 reports on identity theft,<sup>1</sup> March 2002 report on the INS's Forensic Document Laboratory,<sup>2</sup> January 2002 report on immigration benefit fraud,<sup>3</sup> May 2000 report on alien smuggling,<sup>4</sup> July 1999 congressional testimony on illegal aliens and fraudulent documents,<sup>5</sup> and April 1999 report on INS's worksite enforcement efforts.<sup>6</sup> We also obtained information from the U.S. Secret Service, the Social Security Administration's Office of the Inspector General (SSA/OIG), the Federal Bureau of Investigation (FBI), the United States Sentencing Commission, and publicly available sources.

---

<sup>1</sup>U.S. General Accounting Office, *Identity Fraud: Information on Prevalence, Cost, and Internet Impact Is Limited*, GAO/GGD-98-100BR (Washington, D.C.: May 1, 1998) and *Identity Theft: Prevalence and Cost Appear to be Growing*, GAO-02-363 (Washington, D.C.: Mar. 1, 2002).

<sup>2</sup>U.S. General Accounting Office, *INS Forensic Document Laboratory: Several Factors Impeded Timeliness of Case Processing*, GAO-02-110 (Washington, D.C.: Mar. 13, 2002).

<sup>3</sup>U.S. General Accounting Office, *Immigration Benefit Fraud: Focused Approach Is Needed to Address Problems*, GAO-02-66 (Washington, D.C.: Jan. 31, 2002).

<sup>4</sup>U.S. General Accounting Office, *Alien Smuggling: Management and Operational Improvements Needed to Address Growing Problem*, GAO/GGD-00-106 (Washington, D.C.: May 1, 2000).

<sup>5</sup>Statement of Richard M. Stana, U.S. General Accounting Office, *Illegal Aliens: Fraudulent Documents Undermining the Effectiveness of the Employment Verification System*, GAO/T-GGD/HHS-99-175 (Washington, D.C.: July 22, 1999), before the Subcommittee on Immigration and Claims, Committee on the Judiciary, House of Representatives.

<sup>6</sup>U.S. General Accounting Office, *Illegal Aliens: Significant Obstacles to Reducing Unauthorized Alien Employment Exist*, GAO/GGD-99-33 (Washington, D.C.: Apr. 2, 1999).

---

### Prevalence of Identity Theft Appears to be Growing

No single hotline or database captures the universe of identity theft victims. Some individuals do not even know that they have been victimized until months after the fact, and some known victims may not know to report or may choose not to report to the police, credit bureaus, or established hotlines. Thus, it is difficult to fully or accurately measure the prevalence of identity theft. Some of the often-quoted estimates of prevalence range from one-quarter to three-quarters of a million victims annually. Generally speaking, the higher the estimate of identity theft prevalence, the greater the (1) number of victims who are assumed not to report the crime and (2) number of hotline callers who are assumed to be victims rather than “preventative” callers. However, we found no information to confirm the extent to which these assumptions are valid.

Nevertheless, although it is difficult to specifically or comprehensively quantify identity theft, a number of data sources can be used as proxies or indicators for gauging the prevalence of such crime. These sources include

- the three national consumer reporting agencies that have call-in centers for reporting identity fraud or theft;
- the Federal Trade Commission (FTC), which maintains a database of complaints concerning identity theft;
- the SSA/OIG, which operates a hotline to receive allegations of SSN misuse and program fraud; and
- federal law enforcement agencies—Department of Justice components, Department of the Treasury components, and the Postal Inspection Service—responsible for investigating and prosecuting identity theft-related cases.

Each of these various sources or measures seems to indicate that the prevalence of identity theft is growing.

---

### Consumer Reporting Agencies: An Increasing Number of Fraud Alerts on Consumer Files

According to the three national consumer reporting agencies, the most reliable indicator of the incidence of identity theft is the number of long-term (generally 7 years) fraud alerts placed on consumer credit files. Fraud alerts constitute a warning that someone may be using the consumer's personal information to fraudulently obtain credit. Thus, a purpose of the alert is to advise credit grantors to conduct additional identity verification or contact the consumer directly before granting credit. One of the three consumer reporting agencies estimated that its 7-year fraud alerts involving identity theft increased 36 percent over 2 recent

years—from about 65,600 in 1999 to 89,000 in 2000.<sup>7</sup> A second agency reported that its 7-year fraud alerts increased about 63 percent in recent comparative 12-month periods; that is, the number increased from 19,347 during one 12-month period (July 1999 through June 2000) to 29,593 during the more recent period (July 2000 through June 2001). The third agency reported about 92,000 fraud alerts<sup>8</sup> for 2000 but was unable to provide information for any earlier year.<sup>9</sup>

**FTC: An Increasing Number of Calls to the Identity Theft Data Clearinghouse**

The federal Identity Theft Act (P.L. 105-318) required the FTC to “log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief” that one or more of their means of identification have been assumed, stolen, or otherwise unlawfully acquired. In response to this requirement, on November 1, 1999, FTC established a toll-free telephone hotline (1-877-ID-THEFT) for consumers to report identity theft. Information from complainants is accumulated in a central database (the Identity Theft Data Clearinghouse) for use as an aid in law enforcement and prevention of identity theft. From its establishment in November 1999 through September 2001, FTC’s Identity Theft Data Clearinghouse received a total of 94,100 complaints from victims, including 16,784 complaints transferred to the FTC from the SSA/OIG. In the first month of operation, the Clearinghouse answered an average of 445 calls per week. By March 2001, the average number of calls answered had increased to over 2,000 per week. In December 2001, the weekly average was about 3,000 answered calls. However, FTC staff noted that identity theft-related statistics may, in part, reflect enhanced consumer awareness and reporting.

<sup>7</sup> These estimates are approximations based on the judgment and experience of agency officials.

<sup>8</sup> The duration of this agency’s fraud alerts can vary from 2 to 7 years, at the discretion of the individual consumer.

<sup>9</sup> An aggregate figure—totaling the number of fraud alerts reported by the three consumer reporting agencies—may be misleading, given the likelihood that many consumers may have contacted more than one agency. During our review, we noted that various Web sites—including those of two of the three national consumer reporting agencies, as well as the FTC’s Web site—advise individuals who believe they are the victims of identity theft or fraud to contact all three national consumer reporting agencies.



---

**SSA/OIG: An Increasing Number of Fraud Hotline Allegations**

SSA/OIG operates a fraud hotline to receive allegations of fraud, waste, and abuse. In recent years, SSA/OIG has reported a substantial increase in calls related to identity theft. For example, allegations involving SSN misuse increased more than fivefold, from about 11,000 in fiscal year 1998 to about 65,000 in fiscal year 2001. A review performed by SSA/OIG of a sample of 400 allegations of SSN misuse indicate that up to 81 percent of all allegations of SSN misuse related directly to identity theft.

According to the SSA Inspector General, the dramatic rise in SSN misuse over the years has resulted partly from opportunities for fraud associated with the status of the SSN as a “de facto” national identifier, which is used by federal and state governments, banks, credit bureaus, insurance companies, medical care providers, and innumerable other industries. For a May 2000 congressional hearing on SSN misuse, the Inspector General’s statement for the record noted that:

“... our office has investigated numerous cases where individuals apply for benefits under erroneous SSNs. Additionally, we have uncovered situations where individuals counterfeit SSN cards for sale on America’s streets. From time to time, we have even encountered SSA employees who sell legitimate SSNs for hundreds of dollars. Finally, we have seen examples where SSA’s vulnerabilities in its enumeration business process [i.e., the process for issuing SSNs] adds to the pool of SSNs available for criminal fictitious identities.”<sup>10</sup>

---

**Federal Law Enforcement: Increasing Indications of Identity Theft-Related Crime**

Although federal law enforcement agencies do not have information systems that specifically track identity theft cases, the agencies provided us with statistics for identity theft-related crimes. Regarding bank fraud, for instance, the FBI reported that its arrests increased from 579 in 1998 to 645 in 2000—and was even higher (691) in 1999. The Secret Service reported that, for recent years, it has redirected its identity theft-related efforts to focus on high-dollar, community-impact cases. Thus, even though the total number of identity theft-related cases closed by the Secret Service decreased from 8,498 in fiscal year 1998 to 7,071 in 2000, the amount of fraud losses prevented in these cases increased from a reported average of about \$73,000 in 1998 to an average of about \$218,000 in 2000.<sup>11</sup>

---

<sup>10</sup>SSA/OIG, Statement for the Record, hearing on SSN misuse before the Subcommittee on Social Security, House Committee on Ways and Means (May 9, 2000).

<sup>11</sup>In compiling case statistics, the Secret Service defined “identity theft” as any case related to the investigation of false, fraudulent, or counterfeit identification; stolen, counterfeit, or altered checks or Treasury securities; stolen, altered, or counterfeit credit cards; or financial institution fraud.

---

The Postal Inspection Service, in its fiscal year 2000 annual report, noted that identity theft is a growing trend and that the agency's investigations of such crime had "increased by 67 percent since last year."

---

**Technology Affords Increased Opportunities for Identity Theft**

Opportunities for identity theft-related criminal activities have been enhanced by growth of the Internet, which increases the availability and accessibility of personal identifying information. According to the FBI:

"The availability of information on the Internet, in combination with the advances in computer hardware and software, makes it easier for the criminal to assume the identity of another for the purposes of committing fraud. For example, there are web-sites that offer novelty identification cards (including the hologram). After downloading the format, fonts, art work, and hologram images, the information can be easily modified to resemble a state-issued driver's license. In addition to drivers' licenses, there are web-sites that offer birth certificates, law enforcement credentials (including the FBI), and Internal Revenue Service forms."<sup>12</sup>

Similarly, the SSA/OIG has noted that, "The ever-increasing number of identity theft incidents has exploded as the Internet has offered new and easier ways for individuals to obtain false identification documents, including Social Security cards."<sup>13</sup>

---

**Aliens Use Fraudulent Documents to Obtain Entry, Employment, and Other Benefits**

Aliens and others have used identity theft or other forms of identity fraud to create fraudulent documents that might enable individuals to enter the country and seek job opportunities. With nearly 200 countries using unique passports, official stamps, seals, and visas, the potential for immigration document fraud is great. In addition, more than 8,000 state or local offices issue birth certificates, driver's licenses, and other documents aliens can use to establish residency or identity. This further increases the number of documents that can be fraudulently used by aliens to gain entry into the United States, obtain asylum or relief from deportation, or receive such other immigration benefits as work permits or permanent residency status.

---

<sup>12</sup>Statement of Lynne A. Hunt, Section Chief, Financial Crimes Section, FBI, hearing on "Internet Fraud: Illegal False Identification Websites," before the Permanent Subcommittee on Investigations, Senate Committee on Governmental Affairs (May 19, 2000).

<sup>13</sup>Statement of Jane E. Vezaris, Deputy Inspector General of Social Security, "The Emergence of Identity Theft as a Law Enforcement Issue in California," before the Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary (Aug. 30, 2000).

Reportedly, large-scale counterfeiting has made employment eligibility documents widely available. For example, in May 1998, INS seized more than 24,000 counterfeit Social Security cards in Los Angeles after undercover agents purchased 10,000 counterfeit INS permanent resident cards from a counterfeit document ring.

#### Attempting Entry into the United States with Fraudulent Documents

Generally, when a person attempts to enter the United States at a port of entry, INS inspectors require the individual to show one of several documents that would prove identity and/or authorize entry. These documents include border crossing cards, alien registration cards, nonimmigrant visas, U.S. passports or other citizenship documents, foreign passports or citizenship documents, reentry permits, refugee travel documents, and immigrant visas.

At ports of entry, INS inspectors annually intercept tens of thousands of fraudulent documents presented by aliens attempting to enter the United States. As table 1 shows, INS inspectors intercepted over 100,000 fraudulent documents annually in fiscal years 1999 through 2001. Generally, about one-half of all the intercepted documents were border crossing cards and alien registration cards.<sup>11</sup>

**Table 1: Number and Type of Fraudulent Documents Intercepted by INS Inspectors, Fiscal Years 1998 through 2001**

Type of document	Fiscal year 1998	Fiscal year 1999	Fiscal year 2000	Fiscal year 2001
Border crossing cards	30,631	30,797	38,650	30,419
Alien registration cards	28,137	33,308	34,120	26,259
Nonimmigrant visas	13,551	18,003	17,417	21,127
U.S. passports and citizenship documents	14,546	22,142	17,703	18,925
Foreign passports and citizenship documents	11,245	14,695	15,047	15,894
Reentry permits and refugee travel documents	271	1,107	153	702
Immigrant visas	790	663	447	597
<b>Total</b>	<b>99,171</b>	<b>120,715</b>	<b>123,537</b>	<b>114,023</b>

Source: INS data.

<sup>11</sup>Border crossing cards are issued to Mexican Nationals who frequently cross the border for business or pleasure. Most cardholders must stay within 25 miles of the border and limit each visit to 72 hours. Alien registration cards, commonly called green cards, are issued to permanent resident aliens.

---

### Attempting to Obtain Employment with Fraudulent Documents

The availability of jobs is one of the primary magnets attracting illegal aliens to the United States. Immigration experts believe that as long as opportunities for employment exist, the incentive to enter the United States illegally will persist and efforts at the U.S. borders to prevent illegal entry will be undermined. The Immigration Reform and Control Act (IRCA) of 1986<sup>13</sup> made it illegal for employers to knowingly hire unauthorized aliens. IRCA requires employers to comply with an employment verification process intended to provide employers with a means to avoid hiring unauthorized aliens. The process requires newly hired employees to present documentation establishing their identity and eligibility to work. From a list of 27 acceptable documents, employees have the choice of presenting 1 document establishing both identity and eligibility to work (e.g., an INS permanent resident card) or 1 document establishing identity (e.g., a driver's license) and 1 establishing eligibility to work (e.g., a Social Security card). Generally, employers cannot require the employees to present a specific document. Employers are to review the document or documents that an employee presents and complete an Employment Eligibility Form, INS Form I-9. On the form, employers are to certify that they have reviewed the documents and that the documents appear genuine and relate to the individual. Employers are expected to judge whether the documents are obviously fraudulent. INS is responsible for checking employer compliance with IRCA's verification requirements.

Significant numbers of aliens unauthorized to work in the United States have used fraudulent documents to circumvent the employment verification process designed to prevent employers from hiring them. For example, INS data showed that about 50,000 unauthorized aliens were found to have used 78,000 fraudulent documents to obtain employment over the 20-month period from October 1996 through May 1998. About 60 percent of the fraudulent documents used were INS documents; 36 percent were Social Security cards, and 4 percent were other documents, such as driver's licenses. Also, we noted that counterfeit employment eligibility documents were widely available. For instance, in November 1998 in Los Angeles, INS seized nearly 2 million counterfeit documents, such as INS permanent resident cards and Social Security cards, which were headed for distribution points around the country.

---

<sup>13</sup>P.L. 99-603, 8 U.S.C. 1324a *et seq.*

---

**Attempting to Obtain  
Other Benefits with  
Fraudulent Documents**

Aliens have also attempted to use fraudulent documents or other illegal means to obtain other immigration benefits, such as naturalization or permanent residency. Document fraud encompasses the counterfeiting, sale, or use of false documents, such as birth certificates, passports, or visas, to circumvent U.S. immigration laws and may be part of some benefit application fraud cases. Such fraud threatens the integrity of the legal immigration system.

Although INS has not quantified the extent of immigration benefit fraud, agency officials told us that the problem was pervasive and would increase.<sup>16</sup> In one case, for example, an immigration consulting business filed 22,000 applications for aliens to qualify under a legalization program. Nearly 5,500 of the aliens' claims were fraudulent and 4,400 were suspected of being fraudulent. In another example, according to an INS Miami District Office official, during the month of January 2001 its investigative unit received 205 leads, of which 84 were facilitator cases (e.g., cases involving individuals or entities who prepare fraudulent benefit applications or who arrange marriages for a fee for the purpose of fraudulently enabling an alien to remain in the United States). In both of these examples, fraudulent documents played a role in the attempts to obtain immigration benefits.

---

**Identity Theft and  
Fraudulent  
Documents Can Be  
Components of  
Serious Crimes**

Federal law enforcement officials have acknowledged that identity theft often is an essential component of many criminal activities, ranging from bank and credit card fraud to international terrorism. At a May 2, 2002, press conference to announce an initiative to crack down on identity theft, the Attorney General said that:

"In addition to the credit card and financial fraud crimes often committed, identity theft is a major facilitator of international terrorism. Terrorists have used stolen identities in connection with planned terrorist attacks. An Algerian national facing U.S. charges of identity theft, for example, allegedly stole the identities of 21 members of a health club in Cambridge, Massachusetts, and transferred the identities to one of the individuals convicted in the failed 1999 plot to bomb the Los Angeles International Airport."

The events of September 11, 2001, have increased the urgency of being able to effectively authenticate the identity of individuals.

---

<sup>16</sup>GAO-02-56 (Jan. 31, 2002).

---

**Alien Smugglers Use  
Fraudulent Documents**

In addition to using identity theft or identity fraud to enter the United States illegally and seek job opportunities, some aliens have used fraudulent documents in connection with serious crimes, such as narcotics trafficking and terrorism. For instance, according to INS, although most aliens are smuggled into the United States to pursue employment opportunities, some are smuggled as part of a criminal or terrorist enterprise.

INS believes that its increased enforcement efforts along the southwest border have prompted greater reliance on alien smugglers and that alien smuggling is becoming more sophisticated, complex, organized, and flexible. In a fiscal year 2000 threat assessment, INS predicted that fraud in obtaining immigration benefits would continue to rise as the volume of petitions for benefits grows and as smugglers search for other methods to introduce illegal aliens into the United States. Also, INS believes organized crime groups will increasingly use smugglers to facilitate illegal entry of individuals into the United States to engage in criminal activities. Alien smugglers are expected to increasingly use fraudulent documents to introduce aliens into the United States.

---

**Conspirator in World Trade  
Center Bombing Used  
Fraudulent Document to  
Enter United States**

In February 1993, a massive explosion at the World Trade Center complex in New York City killed 6 people and injured approximately 1,000 others. According to a report by the Department of Justice's Office of the Inspector General:

"One of the conspirators in the World Trade Center bombing entered the country on a photo-substituted Swedish passport in September 1992. The suspect used a Swedish passport 'expecting to pass unchallenged through the INS inspection area at New York's Kennedy Airport—since an individual bearing a valid Swedish passport does not even need a visa to enter the United States.' When the terrorist arrived at John F. Kennedy International Airport (JFK), an INS inspector suspected that the passport had been altered. A search of his luggage revealed instructional materials for making bombs; the subject was detained and sentenced to six months' imprisonment for passport fraud. In March 1994 he was convicted for his role in the World Trade Center bombing and sentenced to 240 years in prison and a \$500,000 fine."<sup>17</sup>

---

<sup>17</sup>U.S. Department of Justice, Office of the Inspector General, *The Potential for Fraud and INS's Efforts to Reduce the Risks of the Visa Waiver Pilot Program*, Inspection Report Number I-99-10 (Mar. 1999).

---

Furthermore, regarding this terrorist incident, a United States Sentencing Commission report noted that, "The World Trade Center defendant used, and was in possession of, numerous false identification documents, such as photographs, bank documents, medical histories, and education records from which numerous false identities could have been created."<sup>14</sup>

---

**FBI and State Department Views on Links between Identity Theft or Fraud and Terrorism**

At a February 2002 congressional hearing, an FBI representative testified that various FBI field offices had begun criminal financial investigative initiatives focusing on fraud schemes having a potential nexus to terrorist financing.<sup>15</sup> The FBI representative's statement for the record included the following point:

"Terrorist financing methods range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been utilized by terrorists and terrorist groups. Traditionally, their efforts have been aided considerably by the use of correspondent bank accounts, private banking accounts, offshore shell banks, ... bulk cash smuggling, **identity theft**, credit card fraud, and other criminal operations such as illegal drug trafficking. (Emphasis added.)

Also, at a March 2002 congressional hearing, a Department of State representative testified that:

"There often is a nexus between terrorism and organized crime, including drug trafficking. ... Both groups make use of fraudulent documents, including passports and other identification and customs documents to smuggle goods and weapons."<sup>16</sup>

---

<sup>14</sup>United States Sentencing Commission, Economic Crimes Policy Team, *Identity Theft Final Report* (Washington, D.C.: Dec. 15, 1999).

<sup>15</sup>Mr. Dennis M. Lormel, Chief, Financial Crimes Section, FBI, Statement for the Record before the Subcommittee on Oversight and Investigations, House Committee on Financial Services (Feb. 12, 2002).

<sup>16</sup>Mr. Rand Beers, Assistant Secretary of State for International Narcotics and Law Enforcement Affairs, Department of State, at a hearing on "Narco-Terror: The Worldwide Connection Between Drugs and Terrorism," before the Subcommittee on Technology, Terrorism and Government Information, Senate Committee on the Judiciary (Mar. 13, 2002).

---

**SSA/OIG Investigating  
Links between SSN Misuse  
and Terrorism**

Since the September 11 attacks, the SSA/OIG has reported increasing its efforts to work with federal, state, and local law enforcement officials to investigate and prosecute SSN misuse, including cases in which SSNs may have been used to facilitate or camouflage terrorist crimes.<sup>13</sup> In its May 2002 report, the SSA/OIG summarized the interim results of a task force investigation ("Operation Safe Travel"), which began in September 2001 when SSA/OIG agents developed information that individuals working at the Salt Lake City International Airport were misusing SSNs for security badge applications and employment eligibility verification:

"Under the direction of the U.S. Department of Justice (DOJ), investigators subpoenaed records for all 9,600 airport employees with security badges to identify instances of SSN misuse. They identified 61 individuals with the highest-level security badges and 125 individuals with lower level badges who misused SSNs. A Federal grand jury indicted 69 individuals for Social Security and INS violations. Sixty-one of the 69 individuals arrested had an SSN misuse charge by the U.S. Attorney. On December 11, 2001, SSA's OIG agents and other members of the Operation Safe Travel Task Force arrested 50 individuals. To date, more than 20 have been sentenced after pleading guilty to violations cited in the indictments. Many are now involved in deportation proceedings. There were other similar airport operations after the Salt Lake City Operation, and more are underway."

In the May 2002 report, the SSA Inspector General noted that identity theft begins, in most cases, with the misuse of an SSN. In this regard, the Inspector General emphasized the importance of protecting the integrity of the SSN, especially given that this "de facto" national identifier is the "key to social, legal, and financial assimilation in this country" and is a "link in our homeland security goal."

---

<sup>13</sup>SSA/OIG, *Social Security Number Integrity: An Important Link in Homeland Security*, Management Advisory Report, A-08-02-22077 (May 2002).



### Efforts to Prevent Identity Theft and Other Forms of Identity Fraud Are Important

In its 1999 study of identity theft, the United States Sentencing Commission reported that SSNs and driver's licenses are the identification means most frequently used to generate or "breed" other fraudulent identifiers.<sup>23</sup> Also, in early 1999, following passage of the federal Identity Theft Act, the U.S. Attorney General's Council on White Collar Crime established the Subcommittee on Identity Theft to foster coordination of investigative and prosecutorial strategies. Subcommittee leadership is vested in the Fraud Section of the Department of Justice's Criminal Division, and membership includes various federal law enforcement and regulatory agencies, as well state and local law enforcement representation. The subcommittee chairman told us that, since the terrorist incidents of September 11, 2001, the subcommittee has begun to focus more on prevention. For example, the chairman noted that the American Association of Motor Vehicle Administrators attended a recent subcommittee meeting to discuss ways to protect against counterfeit or fake driver's licenses.

The May 2002 SSA/OIG report, cited previously, stated that, "while the ability to punish identity theft is important, the ability to prevent it is even more critical." In this regard, the Inspector General noted that effective protections to prevent SSN misuse must be put in place at three stages—before issuance of the SSN, during the life of the number holder, and upon that individual's death.

Other prevention efforts designed to enhance technologies in support of identification and verification functions include the following:

- The Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173), signed by the President on May 14, 2002, requires that all travel and entry documents (including visas) issued by the United States to aliens be machine-readable and tamper-resistant and include standard biometric identifiers by October 26, 2004. Also, the act requires the Attorney General to install machine readers and scanners at all U.S. ports of entry by this date so as to allow biometric comparison and authentication of all U.S. travel and entry documents and of all passports issued by visa waiver countries.
- The USA Patriot Act (P.L. 107-56), signed by the President on October 26, 2001, has various provisions requiring development of technology

<sup>23</sup>United States Sentencing Commission, Economic Crimes Policy Team, *Identity Theft Final Report* (Washington, D.C.: Dec. 15, 1999).

---

standards to confirm identity. Under the legislation, the Department of Commerce's National Institute of Standards and Technology is to develop and certify accuracy standards for biometric technologies.

In November 2001, to support implementation of the USA Patriot Act, the Executive Board of the InterNational Committee for Information Technology Standards<sup>25</sup> announced establishment of a technical committee to help accelerate biometric standardization. In its announcement, the Executive Board noted that biometric standards will permit faster deployment of better security solutions and also greatly help in the prevention of identity theft.

---

Chairman Smith and Chairman Gekas, this concludes my prepared statement, I would be pleased to answer any questions that you or other members of the subcommittees may have.

---

## Contacts and Acknowledgments

For further information regarding this testimony, please contact Richard M. Stana at (202) 512-8777 or Danny R. Burton at (214) 777-5600. Individuals making key contributions to this testimony included Michael P. Dino, Bonnie Hall, Shirley A. Jones, Robert J. Rivas, Ronald J. Salo, and Ellen T. Wolfe.

---

<sup>25</sup>The InterNational Committee for Information Technology Standards is sponsored by the Information Technology Industry Council, a trade association representing the leading U.S. providers of information technology products and services. Also, the InterNational Committee is accredited by, and operates under rules approved by, the American National Standards Institute. These rules are designed to ensure that voluntary standards are developed by the consensus of directly and materially affected interests.

Mr. GEKAS. We thank you, Mr. Stana, and we turn to Mr. Edmund Mierzwinski.

**STATEMENT OF EDMUND MIERZWINSKI, CONSUMER PROGRAM DIRECTOR, STATE PUBLIC INTEREST RESEARCH GROUPS**

Mr. MIERZWINSKI. Thank you, Mr. Chairman. I'm Ed Mierzwinski. I'm with the national office of the State Public Interest Research Groups. We're consumer environmental advocacy organizations—nonprofit, nonpartisan—active around the country.

We have been looking at the problem of identity theft for as long as anybody. The State PIRGs put out our first report on the problem consumers face with identity theft in 1996, and since then we've put out two subsequent reports on identity theft.

As the previous witnesses have documented, it's very difficult to get a handle on the costs of identity theft and the magnitude of identity theft in the country. And our estimates, based on talking to all leading experts and based on looking at all available data, are that as many as half a million Americans a year are victims of identity theft. The Federal Trade Commission is now tracking identity theft as a result of the 1998 legislation, and it is part of several intergovernmental task forces. The Federal Trade Commission now posts on its Web site annualized statistics broken down by city, and by State in some instances, on the growth of identity theft.

The big problem that consumers have had with identity theft—and this is—of course, what I'm referring to first here is financial identity theft, the theft of documents to obtain credit in my name—is, of course, that for many, many years the financial industry denied that it was a problem, they continue to deny that it is a problem, and they also continue to deny that consumers are the victim. Because as most of you know, if your credit card is stolen, you're only liable for the first \$50.

Well, our report that we summarize extensively in my testimony documents that in fact the out-of-pocket costs to consumers, the loss of face, the loss of dignity, the hundreds of hours on the telephone, the thousands of dollars in litigation costs trying to regain their good name are serious costs to society. And it's high time, in our view, that the Congress imposes strict restrictions on creditors and credit bureaus who use sloppy practices to give somebody credit.

If I want to obtain a copy of my credit report, I need to provide, in certain circumstances, a Xerox copy of my utility bill, a Xerox copy of my driver's license, the name of my—my mother—my mother's maiden name, excuse me—my current address, my recent—most recent addresses for the last 5 years. And even then, the credit bureau gives me trouble getting a copy of my credit report.

If you apply for credit in my name and you know my Social Security number, you'll get credit. That's all you need, this sloppy Social Security number. No offense—I don't mean to disparage the agency. I'm referring to the sloppy use of the Social Security number in private enterprise and the easy availability of the Social Security number on the Internet makes it easy for these identity thieves.

So our first recommendation would be to impose greater duties on creditors and credit bureaus to do a better job of determining the authenticity of applicants for credit.

Second, get the Social Security number out of general circulation. Make it a crime to publicly display it. Mr. Shaw has some very strong legislation on limiting uses of the Social Security number and preventing coercion of a consumer's Social Security number to ob—to do business with him.

And third, make it easier for consumers to sue credit bureaus. And there are two bills before the Committee that would extend the statute of limitations for an identity theft victim to sue credit bureaus, following a bad Supreme Court decision in November that limited that right to only 2 years after the crime.

On the important matter of terrorism and identity theft that the Committee is deliberating on with a number of hearings, I simply want to say that in—in our view, some of the solutions that have been proposed as solutions to the terrorism problems are not solutions to the identity theft problem.

First of all, national identity cards will not solve the identity theft problem. I don't need a driver's license, I don't need a card to get credit in your name. All I need to know is your Social Security number.

Second, the more high-tech the card, it'll cost more than \$100, as they may be paying today, but you'll have a lot of false-positive cards out there.

Second, imposing restrictions on the ability of immigrants to obtain driver's licenses won't solve the identity theft problem. And as the National Immigration Law Reform Institute and the American Civil Liberties Union and the National Council of La Raza have pointed out, immigrants without driver's license will simply fuel a market for illegal identity documents or they'll drive without licenses, increasing insurance costs for everyone else.

And finally, I would point out that in the view of many experts, biometrics is not a solution to identity theft. Facial recognition and fingerprint identification systems don't adequately do the job.

My written testimony goes into a number of details on these and other matters. Thank you very much.

[The prepared statement of Mr. Mierzwinski follows:]

#### PREPARED STATEMENT OF EDMUND MIERZWINSKI

Chairmen Smith and Gekas, Representatives Scott and Jackson Lee, members of the subcommittees: Thank you for the opportunity to present the views of the U.S. Public Interest Research Group<sup>1</sup> on solving the problem of identity theft.

#### SUMMARY

As you know, the problem of identity theft has been growing rapidly throughout the 1990s. The state PIRGs released our first report on the problem in 1996. At the time, it was difficult to quantify the magnitude of the problem, since creditors and credit bureaus compiled data in different ways and the disparate government agencies investigating the crimes did not have the resources to work together. Nevertheless, in response to numerous indicators that identity theft was epidemic, several

<sup>1</sup>U.S. Public Interest Research Group (U.S. PIRG) is a non—profit non-partisan public interest advocacy group that serves as the national office for state PIRGs around the country. <<http://www.uspirg.org>>

states,<sup>2</sup> and then, in 1998, the Congress, criminalized identity theft. The 1998 federal identity theft act<sup>3</sup> also required the Federal Trade Commission to develop an identity theft clearinghouse, both to assist consumers and to coordinate inter-governmentally.

Since March 2000, the FTC has begun to release detailed data on the impact of identity theft that dovetail with the findings of our reports.<sup>4</sup> Identity theft experts now estimate that as many as 500,000 or more Americans have their identity stolen each year.<sup>5</sup> Increasingly, it appears that identities are being stolen to be used not only for financial gain, but to use in commission of other criminal acts.<sup>6</sup>

Unfortunately, the data show that criminalization has not significantly slowed the identity theft crime wave. In our view, greater effort must be paid to reining in the practices of creditors and credit bureaus that lead to or abet identity theft.

We would like to make the following key points:

- First, identity theft is a fast growing crime and criminalization is only part of the solution. Identity theft criminalization does not appear to have slowed the growth of identity theft. Creditors (banks, mortgage companies, department stores, etc) and credit bureaus (Experian, Equifax and Trans Union) must improve both their credit granting practices—to reduce the incidence of identity theft—and their treatment of identity theft victims—to make it easier for these victims to clear their good names and re-enter the financial world. Legislation is necessary to coerce these recalcitrant firms, which generally consider a “few” mistakes and a few lawsuit settlements the cost of doing business while they ignore the real costs, both tangible and intangible, to victims. Unless banks, department stores and credit bureaus are forced by law to help prevent identity theft, they will continue in their sloppy credit-granting practices, they will continue to dismiss the problem of identity theft with their public relations campaigns<sup>7</sup> and they will continue to reject the massive impact identity theft has on its consumer victims.
- Second, misuse, over-use and easy access to Social Security Numbers helps drive the identity theft epidemic. Fundamentally, this nation needs to wean the

<sup>2</sup> See chart “STATE IDENTITY THEFT LAWS” [from New York Senate Majority Task Force On Privacy, March 2000, <<http://www.senate.state.ny.us/Docs/nyspriv00.pdf>>] Arizona Ariz. Rev. Stat. Sect. 13-2708, Arkansas Ark. Code Ann. Sect. 5-37-227, California Cal. Penal code Sect. 530.5, Connecticut 1999 Conn. Acts 99, Georgia Ga. Code Ann. Sect. 121, Idaho Idaho Code Sect. 28-3126, Illinois 720 ILCS 5/16/G, Iowa Iowa Code Sect. 715A8, Kansas Kan. State Ann. Sect. 21-4108, Maryland Md. Ann. Code art. 27 sect. 231, Massachusetts Mass. Gen. Laws ch. 266 Sect. 37B, Mississippi Miss. Code Ann. Sect. 97-19-85, Missouri Mo. Rev. State Sect. Sect. 570.223, New Jersey N.J. State Ann. Sect. 2C:21-17, North Dakota N.D.C.C. Sect. 12.1-23-11, Ohio Ohio Rev. Code Ann. 2913, Oklahoma Okla. Stat. Tit. 21, Sect. 1533.1, Tennessee Tenn. Code Ann. Sect. 39-14-150, Texas Tex. Penal Code Sect. 32-51, Washington Wash. Rev. Code Sect. 9.35, West Virginia W. Va. Code Sect. 61-3-54, Wisconsin Wis. Stat. Sect. 943.201 *Source: ID Theft: When Bad Things Happen To Your Good Name. FTC, February 2000.*

<sup>3</sup> Identity Theft Assumption and Deterrence Act of 1998, PL 105-318 (10/30/98), criminalized identity theft and established the Federal Trade Commission as a national identity theft clearinghouse. It was based on HR 4151 (Shadegg-R-AZ) and S. 512 (Kyl-R-AZ). The law is found in the U.S. Code at 18 USC 1028.

<sup>4</sup> See <http://www.ftc.gov/bcp/workshops/idtheft/trends-update-2001.pdf> “Identity Theft Complaint Data January-December 2001 and <http://www.consumer.gov/sentinel/images/charts/idtheft01.pdf> “Identity Theft Victim Complaint Data January-December 2001” for the most up-to-date published FTC data.

<sup>5</sup> Personal communication, Beth Givens, Director Privacy Rights Clearinghouse. See <http://www.privacyrights.org>, 23 June 2002, who estimates 500,000 identity theft victims each year based on her analysis of data provided to government agencies by credit bureaus. These numbers are buttressed by recent FTC data that the commission receives about 80,000 complaints each year. Our estimate is that only 5-10% of victims complain to the government. For details of all available estimates, see report and testimony by U.S. General Accounting Office, GAO-02-424T (testimony) and GAO-02-363 (report) “Identity Theft: Prevalence and Cost Appear To Be Growing,” March 2002.

<sup>6</sup> According to A PIRG/Privacy Rights Clearinghouse survey of identity theft victims, “In 15% of the cases, the thief actually committed a crime and provided the victim’s information when he or she was arrested.” See *Nowhere To Turn*, May 2000, CALPIRG/Privacy Rights Clearinghouse. <<http://www.privacyrights.org/ar/idtheft2000.htm>> or <<http://calpirg.org/CA.asp?id2=3683&id3=CA&>>

<sup>7</sup> See, for example, the recent opinion piece by Oscar Marquis in the *American Banker*, 17 May 2002, claiming that estimates of identity theft over-state the problem. Marquis was until recently the long-time general counsel for the Trans Union credit bureau. He has recently joined Hunton and Williams, a law and lobbying firm that is one of numerous financial-industry affiliated organizations that are publishing “reports” and other polemics in opposition to strict privacy protection laws. See, for a rebuttal to these industry-funded materials, “Privacy, Consumers, and Costs,” March 2002, by Robert Gellman. Available at <http://www.epic.org/reports/dmfprivacy.html>

private sector of its over-reliance on Social Security Numbers (SSN) as unique identifiers and database keys. Creditors issue credit based on a match between an applicant's SSN and a credit bureau SSN, with no additional verification in many cases that the applicant is actually the consumer whose credit bureau file is accessed.

In addition to emphasizing these two main points on identity theft, we would also like to make the following brief comments regarding certain other policy proposals that have been mentioned as solving identity theft:

- First, national identity cards are no solution to the identity theft problem and may make it harder for identity theft victims to clear their names, since a thief with a good identity document in your name can continue to wreck your name. To obtain a driver's license, typically a person presents a birth certificate and maybe an SSN (both can be bought or forged). All the card does is certify that the name and SSN are for the same name. That name is the name claimed by the person standing in front of a clerk. It verifies that is who they say they are—not *who they really are*. Many criminals have false IDs, in the name of another person. National ID cards would presumably be more high-tech, but could still be forged. Again, in addition to their other flaws, national ID cards would not stop identity theft.
- Second, imposing restrictions on the ability of immigrants to obtain drivers' licenses won't solve the identity theft problem. If anything, preventing immigrants from obtaining drivers' licenses means only that they will drive without insurance and their need for identity documents will help fuel the market for more false or illegal identity documents.<sup>8</sup>
- Third, biometrics is no panacea to the identity theft problem. Fingerprint readers have reportedly been spoofed by a researcher using gelatin, the primary ingredient in Gummy Bears.<sup>9</sup> The American Civil Liberties Union (ACLU)'s critique of facial recognition systems includes links to a Department of Defense report finding flaws in facial identity systems.<sup>10</sup> In recognition of these limitations, the Enhanced Border Security and Visa Entry Reform Act of 2001, S. 1749, requires (Section 102(c)(2)) that an independent agency, the National Institute on Standards and Technology (NIST), verify that biometric proposals actually work.

While we are sensitive to the critical need for federal and state governments to take action to respond to and prevent future outbreaks of terrorism, we do not believe that national ID and driver's license policy solutions proposed as a result of 9/11 will help stop identity theft.<sup>11</sup>

#### ANALYSIS OF THE PROBLEM OF IDENTITY THEFT:

*Identity theft is a fast growing crime:* In May 2000, CALPIRG and the Privacy Rights Clearinghouse released a joint survey of identity theft victims. This testimony summarizes the findings of that survey of victims. Less than half of the respondents felt that their cases had been fully resolved, and those with unsolved cases have been dealing with the problem for an average of four years. Victims estimated that they spent an average of 175 hours and \$808 in additional out-of-pocket costs to fix the problems stemming from identity theft.

*Types of Identity Theft:* Experts divide financial identity theft into two main categories. "True name" fraud occurs when someone uses pieces of a consumer's personal identifying information, usually a Social Security number (SSN), to open new accounts in his or her name. Thieves can obtain this information in a variety of ways, from going through a consumer's garbage looking for financial receipts with account numbers and SSNs, to obtaining SSNs in the workplace, to hacking into computer Internet sites, or buying SSNs online.

<sup>8</sup>There are numerous other problems such as a ban on obtaining drivers licenses would create, which are not directly the subject of this hearing. For example, the number of uninsured drivers would increase dramatically, raising rates for all drivers. For a more detailed treatment of the issue, see Michele L. Waslin, *Safe Roads, Safe Communities: Immigrants and State Driver's License Requirements*, National Council of La Raza (NCLR) Issue Brief No. 6, May 2002, available at <http://www.nclr.org/policy/briefs/drivers—license—issue—brief—6.pdf>.

<sup>9</sup>See "Fun With Fingerprint Readers," summarizing work by Japanese cryptographer Tsutomu Matsumoto, web-posted at <http://www.counterpane.com/crypto-gram-0205.html> by Bruce Schneier, editor, *Crypto-Gram Newsletter*, 15 May 2002.

<sup>10</sup>See <http://www.aclu.org/issues/privacy/facial—recognition—faq.html>

<sup>11</sup>We encourage the committee to review the work of the ACLU and National Council of La Raza, among others, in its determination of whether these proposals would help stop terrorism.

“Account takeover” occurs when thieves gain access to a person’s existing accounts and make fraudulent charges. Regardless of the types of fraud committed or the amount of money taken fraudulently, victims indicate that stress, emotional trauma, time lost, and damaged credit reputation—not the financial aspect of the fraud—are the most difficult problems they face. One victim from Nevada explained to us, “this is an extremely excruciating and violating experience, and clearly the most difficult obstacle I have ever dealt with.”

Increasingly, thieves are also committing other crimes using the names generated from identity fraud. In the PIRG/PRC survey, thieves committed various other types of fraud with the respondents’ information, including renting apartments, establishing phone service, obtaining employment, failing to pay taxes, and subscribing to online porn sites. In 15% of the cases, the thief actually committed a crime and provided the victim’s information when he or she was arrested. A growing problem for victims is that thieves who have rented apartments or purchased homes using fraudulent identities are filing for bankruptcy in the victim’s name, with the intention of seeking a mandatory stay against eviction or foreclosure. The false public record bankruptcies are difficult for victims to remove.

*Results of the PIRG/Privacy Rights Clearinghouse Survey of Identity Theft Victims*

The California Public Interest Research Group and the Privacy Rights Clearinghouse have been helping victims of identity theft for years through advocacy, free guides, hotlines, and monthly support group meetings. We have talked to thousands of victims over the phone, through letters and electronic mail, and in person, hearing new, unique and horrifying experiences every day. But so far there have been little in-depth data collected on the specific problems that victims face or on the specific gaps in law enforcement efforts and credit industry practices that make cleaning up a stolen identity such a time-consuming and seemingly impossible task.

In the spring of 2000, CALPIRG and Privacy Rights Clearinghouse sent surveys to victims who had recently contact our offices, and published a report based on the findings, entitled “Nowhere To Turn: Victims Speak Out on Identity Theft.”<sup>12</sup> The report followed up on CALPIRG’s groundbreaking identity theft reports<sup>13</sup> released in 1996 and 1997, and on the pioneering work of the Privacy Rights Clearinghouse in assisting victims and drawing attention to their plight. Both organizations have also worked with victims to find ways that they can help themselves, because until the Federal Trade Commission established its clearinghouse, there was no government agency that made identity theft solutions its priority.<sup>14</sup>

The data pinpoint the failure of law enforcement, government, and the credit industry to address the root causes of identity theft. By not changing their procedures, these stakeholders have both helped perpetuate identity theft and have made it difficult for victims to resolve their cases expeditiously. Although each identity theft case is different, we have been able to identify patterns and trends in the victims’ responses. The survey data also verify that the stories in the news on identity theft are not extreme cases in which an unlucky victim has had an unusually bad experience. As one victim from California stated, “It was as terrible as all the books and articles say it is.”

- Forty-five percent (45%) of the victims consider their cases to be solved; and it took them an average of nearly two years, or 23 months, to resolve them. Victims (55%) in the survey whose cases were open, or unsolved, reported that their cases have already been open an average of 44 months, or almost 4 years.
- Three-fourths, or 76%, of respondents were victims of “true name fraud.” Victims reported that thieves opened an average of six new fraudulent accounts; the number ranged from 1 to 30 new accounts.
- The average total fraudulent charges made on the new and existing accounts of those surveyed was \$18,000, with reported charges ranging from \$250 up to \$200,000. The most common amount of fraudulent charges reported was \$6,000.

<sup>12</sup>The full report, “Nowhere To Turn,” by CALPIRG and the Privacy Rights Clearinghouse, May 2000, is available at <<http://www.pirg.org/calpirg/consumer/privacy/idtheft2000/>>

<sup>13</sup>“Theft of Identity: The Consumer X-Files”, CALPIRG and US PIRG, 1996 and “Theft of Identity II: Return to the Consumer X-Files”, CALPIRG and US PIRG, 1997. See <<http://www.pirg.org/reports/consumer/xfiles/index.htm>>

<sup>14</sup>In 1999 the Federal Trade Commission established a clearinghouse to assist victims of identity theft and document their cases in a database. This endeavor is a result of a new federal law, “The Identity Theft and Assumption Deterrence Act of 1998” (18 USC 1028), implemented in 1999. The FTC maintains a toll-free telephone number for victims, 877-IDTHEFT, as well as a web site, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

- Victims spent an average of 175 hours actively trying to resolve the problems caused by their identity theft. Seven respondents estimated that they spent between 500 and 1500 hours on the problem.
- Victims reported spending between \$30 and \$2,000 on costs related to their identity theft, not including lawyers' fees. The average loss was \$808, but most victims estimated spending around \$100 in out-of-pocket costs.

Victims most frequently reported discovering their identity theft in two ways: denial of either credit or a loan due to a negative credit report caused by the fraudulent accounts (30%) and contact by a creditor or debt collection agency demanding payment (29%).

- Victims surveyed reported learning about the theft an average of 14 months after it occurred, and in one case it took 10 years to find out.
- In one-third (32%) of the cases, victims had no idea how the identity theft had happened. Forty-four percent (44%) of all the victims had an idea how it could have happened, but did not know who the thief was. But in 17% of the cases, someone the victim knew—either a relative, business associate, or other acquaintance—stole his or her identity.
- Victims reported that all of the credit bureaus were difficult to reach, but the hardest one to get in touch with, and the one about which most negative comments were made, was Equifax. Over one-third of the respondents reported not being able to speak with a “live” representative at Equifax or Experian despite numerous attempts. Less than two-thirds felt that the credit bureaus had been effective in removing the fraudulent accounts or placing a fraud alert on their reports. Despite the placement of a fraud alert on a victim's credit report, almost half (46%) of the respondents' financial fraud recurred on each credit report.<sup>15</sup>
- All but one of the respondents contacted the police about their cases, and 76% of those felt that the police were unhelpful. Law enforcement agents issued a police report less than three-fourths of the time, and assigned a detective to the victims' cases less than half of the time. Despite the high rate of dissatisfaction with law enforcement assistance, 21% of the victims reported that their identity thieves had been arrested, often on unrelated charges.
- Thirty-nine percent (39%) of the victims reported contacting the postal inspector about their cases, and only 28% (7 out of 25) of those respondents found the post office helpful. Only four of the respondents reported that the postal inspector placed a statement of fraud on their name and address.
- Forty-five percent (45%) of the respondents reported that their cases involved their drivers' licenses. For example, the license had been stolen and used as identification, or the thief had obtained a license with his or her picture but containing the victim's information. Fifty-six percent (56%) of the respondents contacted the Department of Motor Vehicles, and only 35% of those found the DMV helpful.
- Forty-nine percent (49%) of the respondents contacted an attorney to help solve their cases. Forty-four percent (44%) of those people found their attorney to be somewhat helpful. Many consumers contacted attorneys at public interest law firms and received advice for free. Attorneys' fees ranged from \$800 to \$40,000.
- Respondents reported that the most common problem stemming from their identity theft was lost time (78% of consumers identified this problem). Forty-two percent (42%) of consumers reported long-term negative impacts on their credit reports, and 36% reported having been denied credit or a loan due to the fraud. Twelve percent (12%) of the respondents noted as a related prob-

<sup>15</sup> When a “fraud alert” is placed on a victim's credit file, the credit bureau reports to credit issuers that the subject of the report is a victim of fraud. The creditor is supposed to contact the victim at the phone number provided in the fraud alert in order to determine if it is an imposter or the rightful individual applying for credit. Obviously, if the credit bureau does not adequately report the presence of an alert, which often happens when only a credit score is reported, or if the credit grantor fails to detect the fraud alert, which is a common experience of victims, the imposter is able to obtain additional lines of credit in the victim's name. Consumer and identity theft experts believe that one way that credit bureaus under-state the magnitude of the identity theft problem is by only calculating the results of consumers who place a 7-year or “permanent” fraud flag on their credit reports. Most consumers are quite unaware that there is even an option to insert a permanent fraud flag and are not routinely offered the chance when they call the credit bureaus and “speak” to their “voice-mail-jail” computer response systems.



lem that there was a criminal investigation of them or a warrant issued for their arrest due to the identity theft.

#### SOLUTIONS TO IDENTITY THEFT:

PIRG's key recommendations to prevent identity theft are the following: (1) Require credit bureaus to provide free credit reports annually on request, as six states already do (Colorado, Georgia, Massachusetts, Maryland, New Jersey, Vermont). (2) Provide victims, as well as other consumers, with the right to block access to their credit reports. (3) Require matching of at least four points of identity, such as exact name and exact address, date of birth, account number and former address, instead of only on Social Security number between credit reports and credit applications. (4) Improve address-change verification. (5) Close the "credit header" loophole that allows Social Security numbers to be sold on the information marketplace, including over the Internet. (6) Take Social Security Numbers out of general circulation. (7) Make it easier to sue credit bureaus and creditors.

*Require a free credit report annually:* Credit bureaus should provide a free report annually on request to detect identity theft early and generally improve the accuracy and transparency of credit reporting. Six states (Colorado, Georgia, Massachusetts, Maryland, New Jersey, Vermont) grant consumers the right to a free credit report annually on request from each of the Big Three credit bureaus—Equifax, Experian and Trans Union. Colorado's law laudably also requires an annual notice from the Big Three national credit bureaus (also known as credit reporting agencies, or CRAs) to all credit-active consumers describing their rights under the law, including their right to a free report annually on request. Georgia allows consumers to obtain two free reports per year.

#### *Require Blocking, Matching and Address Verification:*

—*Improve Change Of Address Notification:* Incredibly, identity thieves often steal mail, including pre-approved credit applications, and then apply for credit at a new address. Alternatively, they apply in department stores for "instant credit" in the victim's name, but at a different address. Creditors routinely grant this credit to the thief. Consumers will benefit from the new address change notification provisions of the Hooley bill.

—*Require Fraud Alert Flags and Blocking:* Past victims often complain to our organizations that the so-called fraud alert flags used by the credit reporting agencies (credit bureaus) are either ineffective, ignored, or not sent to report requesters. The Hooley bill and Senate proposals would make such notification a requirement, even if the CRA were providing information for the establishment of a credit score. Currently, no requirement in law requires that either credit score models or credit decision makers relying on credit reports take the presence of fraud flags into account. Importantly, the Hooley provision would prevent the issuance of credit on any account with a fraud flag unless the creditor confirms the identity of the consumer and the particular consumer has actually authorized the issuance of credit. Essentially, this fraud flag provision implements in a very effective way one of our most important recommendations: it empowers consumers to control access to their credit reports. We call that "the right to block." Although the credit reporting industry is generally subject to strong information practice rules (relative to other industries that maintain databases on consumers) credit reports can generally be obtained without consumer consent. All a requester needs is a "permissible purpose." The Hooley fraud flag provision gives victims a strong right to block, or control access to their reports. The provision is highly appropriate, since victims often become repeat victims.

—*Require Matching:* Creditors grant credit on the basis of a match between a name and an SSN to the same or similar name and SSN on a positive credit report. Matching should be required on at least four points of correspondence, including on several items that an identity thief might not readily know. One encouraging sign is that the credit bureaus are finally experimenting with systems that don't match unless the application includes at least one "out-of-wallet" identifier that an identity thief would not have easy access to. Matching on a minimum of 4 points of correspondence should be the law.

*Close the "credit header loophole:"* When it obtained a consent decree with one credit bureau, TRW (now Experian), in 1994 that properly prohibited target marketing from credit reports, the FTC made a serious mistake. It defined certain sensitive personal demographic information contained in credit reports (name, address, phone number, previous address, date of birth, Social Security Number) as exempt from the definition of credit report. Under this loophole, the credit bureaus devel-

oped a lucrative traffic in “credit headers,” which included the demographic information found in a credit report that is not associated with a specific credit trade line or public record. The fly-by-night information broker websites that sell Social Security Numbers to identity thieves and stalkers have generally obtained the Social Security Numbers from credit header data.

Two recent court actions helped to protect privacy. First, in March 2000, in an order against Trans Union,<sup>16</sup> the FTC narrowed the definition of credit header. It removed dates of birth from credit headers, since age is a determinant of credit-worthiness. It stated that since credit scoring and other credit decisions use age, then age information could only be sold by credit bureaus as part of a full credit report. Generally, the use of credit reports is subject to numerous restrictions to protect privacy and avoid misuse. The use of credit headers is not.

Recently, the Supreme Court denied Trans Union’s petition to review the DC Circuit’s April 2001 decision in *Trans Union vs. FTC*, upholding that 2000 FTC order holding that the FCRA banned the use of credit reports for marketing purposes. That order also removed dates of birth from credit headers.

Although the industry continues a series of unsuccessful appeals, also in April 2001, a court upheld the final Gramm-Leach-Bliley financial privacy rules issued in 2000 by the FTC and 5 other federal financial agencies, which defined Social Security Numbers as non-public personal information. That decision was upheld on summary judgment on 30 April 01 by U.S. District Court Judge Ellen Huvelle.

The result of the district court’s strong ruling, which we expect to be continue to be upheld, is that credit bureaus cannot share credit header information (*including Social Security Numbers*) obtained from financial institutions, since the financial institutions have failed to provide consumers with notice of this information sharing practice and the right to opt-out of nonaffiliated third party sharing, as required by the Gramm-Leach-Bliley regulations. However, if banks and other financial institutions modify their defective privacy notices to describe this sharing, the protection will then only apply to consumers who exercise their right to opt-out. Banks have generally not disclosed their sale and sharing of SSNs, for fear this would increase the opt-out rate, which they have intentionally kept low by confusing consumers with poorly written opt-out notices.

While this is a very strong, pro-privacy decision, we believe that it still makes sense for the Congress to enact legislation closing the credit header loophole by statute. Even if Gramm-Leach-Bliley continues to be upheld, ultimately, consumers would have to exercise their modest opt-out rights to gain protections they should have by law.

The Shaw credit header ban proposal in HR 2036 eliminates the need for consumers to deal with the opt-out nonsense financial companies require of them to protect the privacy. It identifies all sensitive personal information in a credit report (everything except name and address) as part of the credit report. So, Social Security Numbers or other non-public information could only be sold or shared with parties that have a permissible purpose to obtain a credit report. This is a strong and important provision to prevent identity theft.

*Take The Social Security Number out of Circulation:* Closing the credit header loophole will reduce access to Social Security Numbers. It will not shut the door completely on their use. Military IDs, insurance and Medicare IDs, college IDs and drivers’ licenses often routinely display Social Security Numbers. Businesses use the SSN as their database key for the same reason Mallory climbed Everest: “Because it is there.” Of course, they have less justification than Mallory did. He was an explorer, creditors and credit bureaus are merely lazy and sloppy. Unless legislation such as the Shaw proposal is enacted, SSNs will continue to be easily available and routinely abused by identity thieves. In addition to its credit header provision, is anti-coercion provision and limits on public display of SSNs will make it harder for identity thieves to obtain the key to a consumer’s financial life.

*Make It Easier To Sue Credit Bureaus and Creditors:* In November, 2001, the Supreme Court raised the bar for identity theft victims, by shortening the FCRA’s statute of limitations to sue credit bureaus to only two years after an error is made. The law also unduly restricts a consumer’s right to sue creditors that make mistakes, restricting most enforcement to agencies.

<sup>16</sup> See <<http://www.ftc.gov/opa/2000/03/transunion.htm>> for the press release accompanying the order of 10 February 2000, released on 1 March 00. “The Commission also found that although demographic information such as name, address, mother’s maiden name and social security number did not meet the definition of a consumer report, age information bears on a consumer’s credit capacity and is used in credit eligibility decisions and therefore does constitute a consumer report.”

## BILLS BEFORE CONGRESS TO STOP IDENTITY THEFT AND HELP VICTIMS:

The primary purpose of our testimony is to address proposals that would stop identity theft and help victims.

—If enacted, the bi-partisan Identity Theft Prevention Act of 2001, HR 3053, as introduced by Rep Hooley, would take several important steps to slow the rise of identity crimes, including imposing new address change requirements on creditors, establishing statutory fraud alert requirements on credit bureaus and allowing consumers to obtain free credit reports on request annually to audit their reports for errors.

—The bi-partisan Social Security Number Privacy and Identity Theft Prevention Act of 2001, HR 2036, introduced by Reps. Shaw, Matsui and others would impose new restrictions on the use and public display of Social Security Numbers. Social Security Numbers are the key used by identity thieves to open your financial lives. The bill includes a strict anti-coercion clause giving consumers the right to say no to most businesses demanding their Social Security Numbers. It would also completely close the door on the so-called “credit header” loophole used by credit bureaus to sell Social Security Numbers outside the strict regulations of the Fair Credit Reporting Act<sup>17</sup> (FCRA). The loophole has been significantly narrowed by recent federal court decisions.<sup>18</sup>

—In November 2001, the Supreme Court, in *TRW vs. Andrews*,<sup>19</sup> limited the rights of victims of both identity theft and other credit bureau mistakes. It held that victims had only two years from the date of an error by a credit bureau, not two years from the consumer’s discovery of the error, to bring a lawsuit against a credit bureau. Bi-partisan legislation, HR 3368, introduced by Reps. Schakowsky and Bachus would reinstate the previous rule of two years from date of discovery of the error by the consumer. Similarly, a bill introduced by Rep. Terry, HR 3387, would extend the statute of limitations to three years following discovery. Both these bills have been referred to both the Judiciary and Financial Services Committees.

According to the FTC, in 2001 at least 16% of identity theft victims did not even know about the crime for over two years. A similar pattern exists for victims of credit bureau errors. This month, Rep. Gary Ackerman, a member of House Financial Services Committee, pointed out during a markup that he will pay thousands of dollars in excess interest on a mortgage due to failing to qualify for a low-interest loan as the result of a 3-year old error on his credit report. Therefore, it is important that the final legislation protect all victims of credit bureau errors, not only identity theft victims.<sup>20</sup>

## CONCLUSION

We appreciate the opportunity to provide the committee with our views on the human impact of the crime of identity theft and the need to impose greater duties on creditors and credit bureaus to stop it from happening. In our view, proposals to strengthen identification documents and require the use of biometric identifiers will not solve the identity theft problem. We look forward to working with the committee on legislation to address the issues raised in the hearing today.

Mr. GEKAS. The gentleman from California, Mr. Issa, is present, as is the gentleman from North Carolina, Mr. Coble; the gentleman from Virginia, Mr. Goodlatte; the gentleman from California, Mr. Gallegly. And I did spot the lady from Pennsylvania for a moment, the lady—Ms. Hart.

<sup>17</sup> 15 USC 1681 *et seq.*

<sup>18</sup> We discuss this further below in the section on credit headers and cite the cases, including the Supreme Court’s decision this month to deny a credit bureau’s petition seeking review of the DC Circuit’s 2001 decision in *Trans Union vs. FTC*, upholding the FCRA’s constitutionality.

<sup>19</sup> See *TRW vs. Andrews*, 13 Nov 2002, No. 00–1045, <http://a257.gakamaitech.net/7/257/2422/13nov20011040/www.supremecourtus.gov/opinions/01pdf/00–1045.pdf> See the amicus brief of U.S. PIRG and other consumer groups, filed in support of identity theft victim Adelaide Andrews, at <http://www.pirg.org/consumer/andrews6.htm>

<sup>20</sup> The Senate Judiciary Committee has marked up S. 1742 (Cantwell) which corrects the Supreme Court decision in *TRW vs. Andrews*, but only for identity theft victims, not all consumers who are victims of credit bureau errors. Any final legislation enacted by the Congress must fix the discovery rule for all consumers, as Rep. Ackerman is not alone. See “Mistakes Do Happen: Credit Bureau Errors Mean Consumers Lose” A 1998 PIRG report on credit bureau errors at <http://www.pirg.org/reports/consumer/mistakes/index.htm>

And now comes the time to subject our witnesses to a bit of cross-examination. It is likely that the floor will call the Members for a series of votes——

Mr. ISSA. They said there'd be no more votes.

Mr. GEKAS. No more votes? Oh, thank you for the information. Is that certain or uncertain? Are we going to debate that now? Are we going to——

Well, we'll subject you to some cross-examination.

Also, Mr. Chabot was here at part—for part of the hearing.

The chair yields itself 5 minutes for a round of questions.

The first question I'd like to ask is to Mr. Stana. Of the ways in which false identity has been successfully used by people who wish to take advantage of us, is there any evidence of false identification to get voter's rights, voter's cards?

Mr. STANA. We haven't looked at that specifically. I've read allegations to that effect, but we have no work that specifically addressed that question.

Mr. GEKAS. Is there anyone studying that at all, do you know?

Mr. STANA. Not at the GAO.

Mr. GEKAS. Well, we might bring it to your attention because after motor-voter, many of us have found instances that resulted in non-citizens gaining the right to vote. And of course everyone who is a non-citizen who votes cancels out one of our votes, who have the legitimate right to do so. And that's a separate problem, but——

Mr. STANA. Yeh, when we spoke with voter registration officials throughout the country in connection with our elections report, we did find that that was a problem that they had said they experienced, but we don't have work on the shelf that directly addresses that issue.

Mr. GEKAS. Yes, Mr. Huse, the—the startling scenario of our terrorists who had—had obtained legitimate Social Security cards, and they got them directly from Social Security Administration, we understand, yet when they were issued these cards they were either tourists or students. How—how could that have happened? How does that occur?

Mr. HUSE. First of all, Mr. Chairman, to be exact, we—we have isolated six of the 19 terrorists that possibly obtained Social Security cards legitimately, but that still is under investigation. It's still not unequivocally—unequivocally established that they did. We do know that all 19 used Social Security numbers. Now, whether they got them with counterfeit documents or what—what have you.

But to answer your sec—part of your—the second part of your question, non-work Social Security numbers were issued in this country for various reasons—some so that people could obtain driver's licenses, a very common practice. Many of the States required that a Social Security number be a precursor identifier to a driver's license application.

That, by the way, has been discontinued as a practice. But prior to September 11, it was a practice.

And other reasons that a non-work number would be issued would be to establish identification at—for students at universities for loan applications.

And lastly, some of these non-citizens would—would obtain work SSNs so that they could work at—at the schools they attended. So there was a variety of loopholes there.

Mr. GEKAS. You mean if they applied for it at work, even if they were non-citizens, the—the Social Security Administration would issue it nonetheless?

Mr. HUSE. Well, they—they—there—there were—there were several exceptions where—where non-citizens could get—

Mr. GEKAS. Yes—

Mr. HUSE [continuing]. A number.

Mr. GEKAS [continuing]. And they are?

Mr. HUSE. Driver's licenses, student identification issues. And I believe those are the only reasons, and if work was authorized for them in the third—

Mr. GEKAS. Like?

Mr. HUSE. For—at a university, a student job—

Mr. GEKAS. Like work visas? Work—direct—

Mr. HUSE. Yes.

Mr. GEKAS [continuing]. Work visas, you're talking about.

Mr. HUSE. Correct. But they would be allowed to work while they were here on a school—on a—on a student visa.

Mr. GEKAS. Is that consistent with what Mr. Stana has found?

Mr. STANA. Generally, yes. I would point out one thing, though, that a number of people at the table here have mentioned, and that's the way individuals work to get driver's licenses and other official documents illegally through official agencies. There are other ways to get these documents that I know are used by aliens. I had occasion to visit the Secret Service office in Dallas not long ago, where a person who had been working there for 1 week made me, with a digital camera and publicly available hardware and software, made me a Nebraska driver's license and a Marine Midland Bank credit card.

And—so you don't need to use a Social Security number or even fill out an application to get these documents. And that should be a cause for great concern.

Mr. McNULTY. Mr. Chairman—

Mr. GEKAS. I was just going to turn—the two fellows that were lingering out in front of what you described, Paul, does that have something to do with that?

Mr. McNULTY. Well, no, I was going to say that we prosecuted a case where the INS forms that you were discussing a moment ago, which authorize work, those forms were stolen and fraudulently filled out, and those were used by a syndicate that was in the business of providing false—providing Social Security numbers to people that didn't have a right to them. By using those forms, they traveled around the country, went into Social Security offices, and got numbers for people who paid for that service.

Mr. GEKAS. The time of the chair has expired. We will turn to the gentleman from Texas, Mr. Smith—after Mrs. Lee, the lady from Texas, who is the Ranking minority Member on the Border Security Subcommittee.

Ms. JACKSON LEE. Thank you, Mr. Chairman. Let me congratulate Mr. McNulty for his new position and the work that he has done, and pose the first question to him on the grounds that I be-

lieve the combination of these two Committees has more or less a focus.

And let me view it from my perspective. And that is that as we proceed toward July 12th, as we focus now on the creation of the homeland security department, as we realize that we must begin looking at practical implementation of solutions, I would hope or believe from my perspective that this is now looking at ways to not only alleviate identity fraud and theft, but really focused on how that impacts the security of the nation.

You did a sweep with a task force that focused, I believe, on individuals with inappropriate documentation at our nation's airports. And so what instruction, legislatively, would you give us—give this Committee, first of all, on that issue as it might relate to individuals wishing to do harm? It seems as if your focus was on felons that were there, in essence under cover.

And let me give a slight bias. I recognize and value that this has happened around the country. In fact, the FAA regulations now, that if you have a past record you can't be around secure areas. And those happen to be our citizens. The down side of that, of course, is if someone fails to acknowledge that they had a felony because they're trying to live a new life. They get themselves in trouble, and what we have is a person with a lost job in a community like my own. That's a separate issue.

But I'm really focusing on these individuals that might be part of a terrorist cell or network who are there in secure areas. Any instruction out of the work that you did on the task force for us, and can we solve the problem with existing laws, as you have done seemingly with this sweep that you did?

Mr. McNULTY. Thank you. The law we used primarily was 18 U.S.C. 1001, which is the—

Ms. JACKSON LEE. Lying on the forms.

Mr. McNULTY. Right. And false information on a Federal form. I think that probably the most significant weakness has been identified by the attorney general in the proposal to increase the penalties for the general false identity statute, which is 18 U.S.C. 1028. And the problem with that statute is that the penalties essentially don't have any effect whatsoever. They are essentially lumped in with the underlying fraud that's occurring, and so there's no incentive whatsoever to prosecute someone for the identity card possession in combination with the false form that's been filled out.

If there was increased penalty, such as—I think it's S. 2541 that's been introduced in the other body—if there was an increased penalty, where there would be an additional penalty as an aggravating factor for the possession of the false identification, in combination with the fraudulent act, I think you would see probably even more prosecutions for this.

Having said that, I mean, I think we're able to use 1001 very effectively. And as those airport cases proved, that act of lying about who you are was prosecuted.

Ms. JACKSON LEE. You would—because you wound up—rounded up a number of individuals and prosecuted, I assume, those individuals that you—and some of them were illegal aliens. Did you

discover any of them with an attempt to perpetrate any terroristic acts?

Mr. McNULTY. We had no evidence that anyone in our various airports that we did arrest and charge was engaged in some terrorist activity. We had 119 indictments between Dulles and Reagan National. And in those cases, the vast majority were either criminal history records that were not disclosed, or false Social Security numbers. We had a handful of fugitives and a relatively, actually, small number of illegal immigrants who were actually charged for immigration fraud.

Ms. JACKSON LEE. And basically they were attempting to have a job and to work and to make an income, as opposed to—

Mr. McNULTY. Well, they were—the most egregious situation was we had a few who were re-entry after deportation. So these are individuals we went to all the trouble to deport. They actually re-entered and then got this job. So they're the more egregious examples of immigration violation.

Ms. JACKSON LEE. Mr. Chairman, I just saw the light green. Is it broken? Because it didn't go—it didn't go to the yellow light in between. Let me just do this, if I can. If I can get an additional—I ask you now for an additional 1 minute. It did not go to the yellow—

Mr. GEKAS. Yes.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. Let me just quickly say to Mr. Stana and Mr. Huse, if I can ask you this question very quickly. Because I do want to get on record my concern, and at this point opposition to a national identification card.

Before September 11, and as you looked at this program globally, did you—was the idea of terrorism a big issue in this identity fraud, or was it a question of an illegal immigrant using the Social Security cards and others? I mean, what was the big issue on this false identification? For both Mr. Huse and Mr. Stana. Thank you very much.

Mr. HUSE. I'll take a quick run first. We've actually been involved for the past 3 years, through a series of 14 audit reports, with our extreme concern—and this is before September 11—about the integrity of the Social Security number and its misuse. A newspaper reporter put it best a few weeks ago in one of his editorials. We conscripted—the American people conscripted the Social Security number to uses way beyond what it was ever intended. And because that's happened, it's put the Social Security Administration and the SSN in a very different place. And that's what we were concerned with, not the terrorism aspects. After September 11, it took on even a different, more focused concern.

Ms. JACKSON LEE. Absolutely. We thank you for that. Mr. Stana, your research investigation.

Mr. STANA. I would say before September 11, most instances of identity theft or identity fraud involved individuals like you and me, people who had lost money, they'd lost time off of their job to try to unwind the situation. As far as fraudulent documents used by aliens to obtain employment, that's been an issue for a long time. And we can debate that in greater detail another time.

I will say, though, that with the rise of alien smuggling, the issue of using fraudulent documents to bring illegal aliens or legally ad-

missible aliens into the country as a part of a criminal enterprise has heightened. And I think that concern was beginning to heighten before September 11. Obviously, since September 11, it has grown even more.

Ms. JACKSON LEE. Thank you very much. Thank you, Mr. Chairman. I see the issues that we need to address. Thank you very much.

Mr. GEKAS. The time of the gentlelady has expired. We turn to the gentleman from Texas, Mr. Smith, for a round of questioning.

Mr. SMITH. Thank you, Mr. Chairman. Mr. McNulty, let me direct my first question to you. In your former testimony, you mentioned that this year you had created a cyber crime unit in Eastern Virginia, particularly to try to combat identity theft. The Subcommittee on Crime, Terrorism and Homeland Security has actually held more hearings—three—on that particular subject than any other. And I was wondering if you could briefly discuss how bad you think the problem is and what Congress should do about it.

Mr. McNULTY. Well, it's a major priority for the department and certainly in the Eastern District of Virginia, where we have such a large presence of high-tech companies. You think about the—just the presence of the Internet backbone in Northern Virginia alone. It was an important thing to do.

So what I did was establish a cyber crime section in the office, of six lawyers who are full-time prosecutors. And one of the important things about doing that is when you have prosecutors who are dedicated to a particular area, they spend their time working with law enforcement agencies to develop cases. Because in a sense, it's kind of entrepreneurial. You're focused on that area of crime, and you're working to build cases.

And the range of cases you can do in cyber crime is enormous—everything from, on the one hand, cyber terrorism and doing things like hacking and disrupting the Internet in various ways—to cyber frauds, where the very things we're talking about today are perpetrated by the use of a computer.

Mr. SMITH. Thank you. That answers my question. Mr. Huse, in your testimony, both written and oral, you mentioned that 8 percent of non-citizens who had requested Social Security numbers submitted fraudulent documents. My question is what has the Social Security Administration done since September 11 to correct that massive problem?

Mr. HUSE. Since September 11, they recognized the problem, and that's a very important step right there. And starting on July 1st in selected cities and then going nationwide in the fall, the Commissioner will establish what she calls enumeration centers.

Mr. SMITH. Well, you're moving toward a solution, then?

Mr. HUSE. Yes, we are.

Mr. SMITH. Okay. I thought you were very direct and candid in your written testimony, that the INS and the IRS, two other agencies, have really failed to protect American lives in not taking actions that they should have. Would you agree with that—my assessment of your testimony?

Mr. HUSE. I think I'd probably state it a little bit more diplomatically, but I think you have a disconnect between three branches of



the Government that, certainly in the past, just caused some of this problem to occur.

Mr. SMITH. One other quick question for you and for Mr. McNulty. How important and how effective do you think biometric identifiers would be if we were to incorporate them into, say, Social Security or other types of identification?

Mr. McNULTY. Go ahead.

Mr. HUSE. I think—

Mr. SMITH. Real briefly, because I want to move on.

Mr. HUSE. I'm very wary of the national identifier—national identity card.

Mr. SMITH. I'm simply talking about making Social Security cards more tamper-proof by using a fingerprint or something like that.

Mr. HUSE. I think—and that's probably why I'm rather reticent. I think we did do this study that Congress asked us to do and reported back, and had a range of options for a stronger Social Security card, starting with, on the low end, different minor enhancements, all the way to biometrics. Those will cost a lot of money, and I don't know that they'll really solve much of this problem.

Mr. SMITH. Okay. Mr. McNulty?

Mr. McNULTY. We need to know that people are who they say they are, but I don't know enough about this subject to have an educated—

Mr. SMITH. Fair enough. Mr. Chairman, I have a minute left, and I'm going to yield it to the gentleman from California, Mr. Gallegly.

Mr. GALLEGLY. I thank the gentleman for yielding.

Mr. Mierzwinski, did I understand you correctly that you do advocate giving driver's licenses to illegal aliens?

Mr. MIERZWINSKI. I didn't say that. I said that the Congress ought not to look at restrictions on driver's licenses to aliens, whether legal or illegal, as a solution to the identity theft problem. I believe that it will simply result in more drivers seeking fraudulent identity and more drivers without insurance.

Mr. GALLEGLY. Do you advocate the issuing of driver's licenses to illegal immigrants?

Mr. MIERZWINSKI. I don't have a position on that.

Mr. GALLEGLY. But they are illegal, so would you advocate any benefits to those that are here illegally, other than their constitutional rights?

Mr. MIERZWINSKI. I would refer, as I did in my testimony, to the work of the National Council of La Raza and the American Civil Liberties Union and the Immigration Rights Forum, that have done some major work on this. I'm not prepared to comment on that.

Mr. GALLEGLY. I appreciate the gentleman's—his comments. I just find it a little perplexing that we would give benefits to people that are illegally here to help perpetuate them being illegally here. I yield back.

Mr. MIERZWINSKI. Very briefly—I'm not trying to dodge the question, sir. Our organization simply does not have a position on that specific issue.

Mr. GEKAS. The time of the gentleman has expired. Although there are votes pending on the floor, we still have 15 minutes to

appear thereon. I will take the prerogative of the gavel to recognize the gentleman from Virginia, Mr. Scott, for a round of questioning. And then after his questioning, we will recess until 5:20.

Mr. Scott is recognized.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. McNulty, you indicated that you had found certain people with false identifications. Did you follow through to see—to evaluate if—how many, if any, posed a serious threat? I mean, there's a difference between cheating to get an ID to get a job and cheating to get—fraudulently getting an ID to blow up buildings and kill people. Did you do an assessment as to who these people were and what kind of threat they posed?

Mr. McNULTY. There was nothing done in the course of the effort to try to do additional investigative work on the individuals. We just recognized the vulnerability of individuals in that situation who could be extorted or could be pressured or coerced to providing some assistance to someone who might have an activity—dangerous activity in mind.

Mr. SCOTT. So the fact that they had a fraudulent ID made them susceptible—

Mr. McNULTY. Possibly.

Mr. SCOTT. Mr. Mierzwinski, you indicated that biometrics with I.D.s was not a—wasn't a good idea. Could you explain what your position there is?

Mr. MIERZWINSKI. Well, I think, Mr. Scott, that the biometrics is being promoted by a number of companies who maybe want to sell biometrics as a solution to the terrible problems that our country faces. But I urge the Committee to take a close examination. One report I've seen, one researcher spoofed a fingerprint reader with gelatin, the active ingredient in Gummy Bears. And the American Civil Liberties Union has documented that even the Department of Defense has some serious problems with facial recognition systems.

The second part of the problem is, if I get a good—

Mr. SCOTT. But by "spoofed," you mean they got a subsequent ID and used that kind of messed up fingerprint to—

Mr. MIERZWINSKI. Right.

Mr. SCOTT [continuing]. Mask the ID—the fact that they were in fact someone else who was also in the data bank?

Mr. MIERZWINSKI. Right. And if you—if you get your fingerprint on an identity card with my name on it, you've got ID that proves you're me, with your fingerprint on it, that you can use to be me. You've essentially created a super-identity document. The biometrics makes your proof that you're me even better. There are some significant problems out there.

Mr. SCOTT. Mr. Huse, what do you need to get a Social Security number, what identification? How do you validate yourself to get a Social Security number?

Mr. HUSE. As a citizen of the United States, you need, you know, of course, proof of birth in this country. And most Social Security numbers are given at birth in this country today, and it's a relatively error-free process. For a non-citizen, of course, you need to prove your place of birth and birth certification with documents that come from—

Mr. SCOTT. You have prove that you have a document that shows that somebody was born in North Carolina on a certain date.

Mr. HUSE. Correct.

Mr. SCOTT. How do you know it's you?

Mr. HUSE. How does Social Security know the——

Mr. SCOTT. How do you know it's the person? You have a person who comes in with a birth certificate. How do you know it's the person?

Mr. HUSE. Well, to—if you're an adult, I mean for adults, Social Security has to verify the authenticity of that document before the number is issued. And it does that.

Mr. SCOTT. Well, I guess my follow-up question——

Mr. HUSE. It's supposed to do that.

Mr. SCOTT. The follow-up question would be how does anything we do today make it more likely that the person who has a Social Security number is actually who he says he is?

Mr. HUSE. That's why I suggested in my testimony, sir, that there really needs to be more interactivity at all levels of government to ensure, in real time, that these documents or these bona fides are valid at the time they're presented.

Mr. SCOTT. How many people are getting false IDs showing they're somebody else, and how many are just trying to get a Social Security card in their own name?

Mr. HUSE. I mean, there's—I don't know the answer to your question. I'm sure there are people who do that, but we don't have—we don't know what we don't know there, if I——

Mr. SCOTT. Okay. Well, let me get in one more question. Mr. Mierzwinski, can you tell me what suing the credit bureaus would do?

Mr. MIERZWINSKI. Well, I think the credit bureaus need to match credit card applications to credit reports on four or five items, rather than simply on the Social Security number. That's the big problem. If I get your Social Security number off the Internet, I can get credit in your name very easily. They need to match on my previous address, they need to use some out-of-wallet identifier, something an ID thief wouldn't know, and they need to use several identifiers in concert together, rather than only the SSN.

Mr. SCOTT. This is a credit bureau?

Mr. MIERZWINSKI. Well, the credit card companies and the credit bureaus need to work together on this. The credit bureaus need to——

Mr. SCOTT. But if they don't do that and give somebody credit in my name and I am inconvenienced and my checking account is raided, they would be financially liable for those losses?

Mr. MIERZWINSKI. Well, the bank would be financially liable for those losses in most cases. The banks typically eat this as a cost of doing business. They think the cost of doing business is less than the cost to society of the half a million victims who've had their lives ruined, and that's the reason the banks haven't upgraded their systems. They're not financially liable enough.

Mr. SCOTT. Mr. Chairman, I'd like unanimous consent that these documents be put in the record.

Mr. GEKAS. Without objection. And the time of the gentleman has expired. The chair revises its estimate as to when the Committee shall return. We now stand in recess until 5:35.

[Recess.]

Mr. GEKAS. The hour of 5:35 having arrived, the recess has expired. But so has the Chairman.

We must under the rules await the presence of two Members, one besides the Chair, in order to proceed. But what I wanted to do was to keep my own record running on—starting on time whenever and wherever possible. So you have to bear the brunt of that, and you have your choice. I can recite sonnets from Shakespeare or sing “Amazing Grace,” whichever you wish me to accomplish.

Keep the decision to yourself, and we will await the arrival of another Member.

[Recess.]

Mr. GEKAS. The time of the recess has expired. Let the record indicate that the gentleman from Mr. Scott along with the Chair constitute the required hearing quorum, and so we shall proceed to quit. [Laughter.]

Mr. GEKAS. I do have one question that I wish to pose. Then I’ll let the gentleman from Virginia, if he wishes to pose another question, and we’ll wind it up that way, pending the arrival of some other Member.

One question, Mr. Huse, that leaps out at us from your testimony, where on page 3 you state that, “Our own work illustrates how wise a decision this is,” that is, to beef up the integrity of the system. “In a recent study, preliminary results indicate that 8 percent (over 100,000) of the 1.2 million [Social Security numbers] assigned to non-citizens during calendar year 2000 were based on invalid immigration documents, which current SSA processes did not detect.”

That’s a lot of people running around without proper documentation. What—are we doing anything about that? That’s the general question. What is the Social Security Administration doing to minimize that?

Mr. HUSE. I previously mentioned some of that, Mr. Chairman.

Mr. GEKAS. Yes, you did.

Mr. HUSE. And it’s a long—it’s a long story, but the—our audit work told us that we had a problem here several years ago, that this isn’t new information that happened just after—because of September 11. We had previously established that there needed to be a much closer connection between the authentication of documents provided by Immigration and Naturalization Service and our processing of SSNs for non-citizens.

In the last Administration, you know, there were a succession of letters sent to INS by the Commissioner of Social Security, and clearly this problem was known.

Since September 11, however, immediately following those horrific events, the Acting Social Security Commissioner at the time, Larry Massanari, established an enumeration task force to fix some of these things. And those are some of the results I alluded to in my testimony.

But they are being addressed now. There are new procedures in place, and there is a commitment now under the aegis of Homeland

Security, under that impetus, for the Immigration and Naturalization Service and SSA to work much closer together to close these—close this gap. I mean, I can be more specific as to what those things are, but—

Mr. GEKAS. When you said that the Social Security Administrator or Acting Social Security Administrator wrote several letters to the INS—

Mr. HUSE. That was the previous Commissioner.

Mr. GEKAS. I understand.

Mr. HUSE. Right.

Mr. GEKAS. What prompted his sending the letters? Did he have something on his desk that showed—

Mr. HUSE. Audit work that we had done that showed that we were continuing to enumerate non-citizens without proper verification of the documents concerned. That was established by our work.

Mr. GEKAS. The Chair now reneges on his first promise to go to Mr. Scott because Mr. Flake appeared, and he has not yet had a chance to ask any questions. So the gentleman from Arizona is recognized for 5 minutes.

Mr. FLAKE. I thank the Chair. I thank the Chair for holding this hearing.

The panel may know that I have a bill that would require States to issue driver's licenses that expire no later than a person—a temporary resident's visa. Right now we have a situation in most States where someone can come to the country on a 6-month visa or a 2-year visa or some kind of student visa and actually go in and get a driver's license for up to, in some States, 44 years if they happen to be 16 years old. That was the practice in my State of Arizona. We have since changed, and I believe seven States now will not issue a license for a period longer than the visa.

Mr. Mierzwinski, you mentioned that any restrictions or any—trying to define who's legal and who is not and the issues of the licenses would simply raise the cost of insurance premiums? Is that your contention?

Mr. MIERZWINSKI. Well, two things, Congressman. And, first of all, my organization hasn't taken a formal position on your legislation. My knowledge on identity theft is the reason I am a witness here. But I have looked at a number of the suggested solutions to the—to some of the problems facing the country, and national ID cards and restrictions of driver's licenses I don't think will solve the problem of identity theft. The problem with restricting driver's licenses I think is clear. It will fuel a market for more fraudulent documents, perhaps even more high-tech fraudulent documents, and, in addition, it may increase drivers' premiums as more people choose to drive without driver's licenses.

Those are some serious issues that I urge you to weigh with your legislation.

Mr. FLAKE. Before I do, can I ask you, is there empirical evidence, is there anything to quantify how many—if having a license actually encourages you to buy insurance? Has there been any study on the topic that you can cite?

Mr. MIERZWINSKI. I don't have that study with me, but I will certainly look into it and get back to your staff.

Mr. FLAKE. Okay. But you're not aware of any study that shows a correlation between having a license for an illegal and actually purchasing insurance?

Mr. MIERZWINSKI. Schoser does not show, but I am in contact with a number of experts on insurance, and I'd be happy to get back to you.

Mr. FLAKE. But you're not aware at this point?

Mr. MIERZWINSKI. Not at this time.

Mr. FLAKE. So any suggestion that it would increase premiums is pure speculation at this point.

Mr. MIERZWINSKI. Well, I've seen it—I've seen it suggested by a number of groups, and it seemed to make sense to me.

Mr. FLAKE. Okay. That's good. Mr. Stana, have you taken a position on the legislation?

Mr. STANA. Well, I think that there isn't one answer to this question. I think what you're proposing would—

Mr. FLAKE. I understand that. I just wondered—

Mr. STANA [continuing]. Certainly help, if it were coupled with some sort of a verification process, a two-stage process that would entail not only a visual inspection but also some sort of inspection that keys back to a database to verify that this individual's visa has expired or driver's license has expired. If you don't do that, just flashing a driver's license or other form of identification could further identity theft not prevent it.

Mr. FLAKE. Good point. Mr. Huse?

Mr. HUSE. I'm going to answer your question obliquely because—I think it's a good idea. We did audit work several years ago, or maybe even less than several years ago, that involved the State—one of your nearby Western States, the State of Utah, where we found that a significant number—and I don't have the number exactly, but I'll be glad to expand that answer in a written response to you—of non-citizens were going into Utah because they could get a driver's license there, a driver's license that had no limits. And that was being used for purposes way beyond operating a motor vehicle on Utah's roads.

Mr. FLAKE. Yes, well, that's—the point of the legislation is that if there is a de facto form of national ID at this point, it's a driver's license.

Mr. HUSE. It's the link between—I think the driver's license and—the combination of the driver's license and the Social Security number together makes the national ID. I think that's a fair statement.

Mr. FLAKE. Thank you, Mr. Huse.

Mr. McNulty, in the last 30 seconds I have?

Mr. McNULTY. I'm here on the Department of Justice ticket, so I don't have a position.

Mr. FLAKE. That's okay with me.

Mr. McNULTY. Well, I don't think we have a position on the issue yet.

Mr. FLAKE. I thank the Chair.

Mr. GEKAS. The time of the gentleman has expired.

It is the intention of the Chair to recognize the gentleman from Virginia, Mr. Scott, for a follow-up question, to be followed by rec-

ognition of the lady from Texas, who will act as the clean-up hitter for another follow-up question or two.

The gentleman from Virginia is recognized.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. McNulty, when a credit card is stolen, the bank will just cut off the credit and do the loss. Is there any attempt to let the credit run to see if you can catch the person?

Mr. McNULTY. That's a very interesting question. We were talking about that during the break. I'm not familiar—

Mr. SCOTT. Okay. Let me follow up. I had that situation where somebody got a card, and they were buying gasoline with it, several times, and that was all they were charging on the card. It seems to me something like that, you have the potential of actually catching somebody.

Mr. McNULTY. Well, two thoughts. First, there are—there are stories about cards continuing to run, and it's a little confusing as to why that is the case. It should be and most people would expect that it would be cut off immediately and it wouldn't be used again. But you do hear that.

Now, why, I'm not sure—it's not clear, and that leads me to my second point, which is that I think there needs to be more enforcement in this area, and it appears as though, from a business perspective, they view this as just a cost of doing business and are not too interested in the enforcement side, at least in terms of bringing cases to law enforcement.

So if that's what they're doing, I'm not sure I see the fruit of that activity.

Mr. SCOTT. Well, when I said let it run, I meant as a sting possibility. Some of the—

Mr. McNULTY. Yes, I hear you.

Mr. SCOTT. Because all of them are preauthorized, so when the number gets in, you know, you could have an alert. Perhaps that may be something we—because it's so expensive to try to do that and the return may not be there that we might want to fund such an operation and think along those lines.

But let me ask one other question to Mr. Huse. For non-citizens trying to get a Social Security card, you have a lot of rigmarole to go through. Is the potential of actually catching somebody using this Social Security number for violent criminal purposes worth all the aggravation you're going to put people through who are trying to get a card legally?

Mr. HUSE. I believe it is. I believe it is, sir.

Mr. SCOTT. And how much would it cost in terms of your administration and people's aggravation to actually tighten it up so that you would know that the person before you is who he is and he's not trying to use it illegally?

Mr. HUSE. Well, I think the Social Security Administration has some idea that by increasing the stewardship side of the focus here so that there is more real-time verification of these documents, which may cause some time delay, that we'll be able to close this loophole. I think the record following September 11 dictates that this be done.

Mr. SCOTT. Does anybody else want to comment?

Mr. STANA. No, I would just say that I think having some form of verification is essential. I think just having a visual verification, whether you're talking about a Social Security card, you're talking about a driver's license, or a border crossing card, isn't sufficient. It's easier to cross the borders in the United States than it is to get in the GAO building, and I'm not so sure that's what should be.

Mr. SCOTT. Well, I mean, the original documents you need, like a birth certificate, how do you get a birth certificate verified?

Mr. STANA. Well, you raise a good point. In your questioning before the break, you asked how do you know that the person who's presenting the birth certificate is really the person who should be presenting that document. And you're raising a good point, and I personally believe that once biometric technology matures, it may afford opportunities to clarify identity than is currently the case.

Mr. HUSE. When a foreign visitor comes to this country, both the State Department and the Immigration and Naturalization Service have a piece in establishing that individual's bona fides and issuing certificate documentation, and that's what Social Security gets. It's that certificate documentation from INS that says it's okay to enumerate this person.

In the ideal, this should be done at the time of entry, and that's really where we're going to go. But that requires perhaps some strengthening of databases and systems that need to be invested in from what we have today. Today we're willing to make the sacrifice to slow things down a little bit to get this done because of the security implications. But in the ideal, it should be done at the time of entry.

Mr. STANA. If I might add briefly, that information that is given to INS and INS uses to create the identity is only going to be as good as the host country systems. Okay? So you're running into a whole other problem.

Mr. GEKAS. The time of the gentleman has expired.

We turn to the lady from Texas.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. I always thought I could be a great baseball player and now here I am.

Let me try to summarize from my perspective—and certainly not represent the view of my colleagues, but I do believe that the thrust of this hearing is to really narrow in the injury that may be done by these false documents and those who would do harm to this country, though I am very concerned of the abuse of the Social Security card because what I know it to be from growing up, it is to say that you are who you are. It's the card that has now become part of my identity to the extent that I could not find that paper card if my life depended on me. But when you ask me for my Social Security number, I do know it, and it has been used through colleges and your transcripts and for any manner of—and I would like us not to have to move away from that. I think it has been very effective. Obviously, it is also used to establish a benefit and that you're the person to get the benefit.

But I would say to you that we need to—even with its broken system, we need to look at the State Department and INS relationship on the visas because that is what happened with the terrorists. They came in on either tourist and/or student visas. They re-



ceived them from their country of origin, and they received them through presenting some sort of documentation. If there has to be any harsh procedures, we've got to wake up and invest in the technology and data sharing that gets them at that point. And we can do no less for this country.

So we need to begin to look at that, and even if—because I have individuals, my constituency, who want to reunite family members, and they've got a mother-in-law who is as innocent as the day is long, but at the visa point, she's being stalled for a variety of reasons. I would like that not to happen. I'd like us to have procedures that can really ferret out the bad guys, and that's technology and documenting who they are, and when I say documenting, looking at fingerprints, how many times they've come in the country, and I think we can do that.

But getting back to the Social Security card, if we can fix that, then explain to me, Mr. Huse—and I must compliment you for what you all have tried to do and proposals, but it looks to me as if you have not yet done some of the things that have been recommended. So I'd like you to comment on obtaining the independent verification from agencies like the INS and State Department when these individuals present you this documentation here in the United States and say, yeah, I'm okay, give me an SSN, give me a number. How do we do that better? How do we—what are you doing? Why haven't you moved into getting that documentation? What do we need? More investment in technology?

Let me just finish. Also, the training of our field office employees who I know are inundated and frustrated, that was one of the issues that we dealt with in the Social Security offices, again, in my community. Frustration, denials keeps you from doing this kind of unique work. I think you need to train people separately from the general run-of-the-mill crowd that comes in and needs their disability because I don't want those people to be cut off from disability or standing in line and confused with others if you're dealing with individuals who do not have citizenship documentation, isolating them, not for the color of their skin or the language they speak, but because they're not a citizen, and have people who are professional.

I'd appreciate it if you would respond to those inquiries, and I guess last is to, like this one, expand the agency's data-matching activities and other Federal, State, and local government entities. And it looks as if you have not yet done that. We've got to do that kind of work, I think, before we can begin to indict ourselves as to the fact that we can't get the job done.

I yield to the distinguished witness.

Mr. HUSE. Thank you. I'm going to take the last part of your question first, and there is significant work to do for us to look at the matching and privacy implications of doing better in sharing data with all of the entities concerned, and that's underway. That's complex and may require some legislative activity on the part of the Congress. That's—we're in a dialogue now with all concerned, to include the Justice Department—

Ms. JACKSON LEE. And it's internally underway? Is that what you're saying? You're looking at that now?

Mr. HUSE. It is underway, that effort.

Ms. JACKSON LEE. All right.

Mr. HUSE. That effort has been joined.

Ms. JACKSON LEE. All right.

Mr. HUSE. The second part of your question—

Ms. JACKSON LEE. Training your employees.

Mr. HUSE. We recognize—actually, Commissioner Barnhart has recognized and has ordered the establishment of and on July 1st we'll start the first of these enumeration centers where we'll take Social Security professionals, INS professionals, members from my staff, and other law enforcement involved, and create a center where enumeration will occur outside of the Social Security field office, which really isn't the place for it in the first place, with all of the new requirements that are called for.

That will be started in several cities on July 1st, and then in the fall it will increase to, I think, 14 other locations around the United States, and eventually it is hoped that will become the way we accomplish this until something better can be done to bring everybody through data sharing and so forth to a better place.

Ms. JACKSON LEE. And you answered the last question, which is the confirmation of the evidentiary documents, and you're going to—I assume this last comment—

Mr. HUSE. It will be done right in one place, which we think is a really effective way to bring everybody to one room where this will be done.

Ms. JACKSON LEE. So you'll take special pains now to make sure these documents are, in fact, legitimate, and you'll have the team—

Mr. HUSE. In real time, right at one place.

Ms. JACKSON LEE. I thank the gentleman.

Mr. GEKAS. The time of the lady has expired.

The time has come for us to dismiss the witnesses with gratitude and to tell them that by their presence here they also submit to written interrogatories on the part of the Members. So we expect that there will be some of that.

Again, we thank you. This meeting stands adjourned.

[Whereupon, at 6 p.m., the Subcommittee was adjourned.]

# A P P E N D I X

## MATERIAL SUBMITTED FOR THE HEARING RECORD



### SOCIAL SECURITY Office of the Inspector General

July 2, 2002

The Honorable Sheila Jackson Lee  
Ranking Minority Member  
Subcommittee on Immigration, Border Security, and Claims  
Committee on the Judiciary  
House of Representatives  
Washington, D.C. 20515

Dear Ms. Jackson Lee:

I appreciate the opportunity you afforded me after the June 25<sup>th</sup> hearing to clarify the planned numbers and timing of the deployment of the Social Security Administration's (SSA) enumeration centers, as well as to summarize Agency plans as set forth by Commissioner Barnhart for improving the security of the Social Security number (SSN).

As I mentioned in my testimony on the 25<sup>th</sup>, SSA has established an Enumeration Working Group to develop and recommend to the Commissioner, both internal and external process changes that will result in strengthening the integrity of the issuance of SSNs. Many of these changes have been made and others are pending implementation in the near term. My office has been a committed partner with SSA in all the activities of that workgroup.

To strengthen the enumeration process, SSA announced last fall that it would:

1. Provide refresher training on enumeration policy and procedures, with emphasis on enumerating non citizens, for all involved staff. Refresher training was begun on December 19 and 20, 2001, and is ongoing.
2. Convene a joint task force between SSA, the Immigration and Naturalization Service (INS), the Department of State (DoS), and the Office of Refugee Resettlement to resolve issues involving enumeration of non citizens, including developing procedures for verifying INS documents before SSN issuance. On January 3, 2002, SSA signed a protocol with the DoS outlining procedures for SSA use of information housed in the Refugee Data Center, which will be used to enumerate refugees. The procedure to verify immigration documents for refugees before assigning an SSN became effective in February 2002. Additionally, the INS has taken several steps to improve the timeliness of its data entry process. Once completed, SSA will begin electronically verifying all non-citizen immigration documents before assigning an SSN. However, it is our understanding that corrections required by INS have been delayed. Therefore, SSA may not begin to implement this policy until late in Calendar Year 2002.

SOCIAL SECURITY ADMINISTRATION BALTIMORE MD 21235-0001

Page 2 – The Honorable Sheila Jackson Lee

3. Eliminate driver's licenses as a reason for a non work number. This initiative has been completed effective March 2002.
4. Provide an alternative to giving out a Numident printout for SSN verification. The Numident file includes information concerning an individual's original and replacement SSN cards issued over their lifetime, as well as identifying information such as date of birth, place of birth, and parent's name. In March 2002, SSA field offices began using the Agency's new NUMI-lite printout, which enables verification of an individual's SSN while providing minimal identity information.
5. Reduced the age by which an individual must personally appear for mandatory interview from age 18 to age 12; require verification of birth records before enumeration for all applicants age 1 and over for original SSNs; and require evidence of identity for all children, regardless of age. This is an ongoing initiative that requires regulatory change. In the interim, SSA is verifying vital statistics on all birth records submitted by U.S. born citizens age 1 or older applying for an SSN with State bureaus.
6. Determine the feasibility of photocopying (or scanning) all documentary evidence submitted with SSN applications. SSA conducted a pilot of this ongoing initiative in February and March 2002.
7. Change the Modernized Enumeration System to provide an electronic audit trail, regardless of the mode used to process SSN applications. This was completed when the audit trail went into production in mid-December 2001.
8. Implemented an on-line verification process for employers to verify SSNs for their employees in April 2002. This initiative is ongoing.

As I stated in my testimony, the Commissioner has recently announced that beginning July 1<sup>st</sup> in selected cities, and this Fall nationwide, SSA will cease the issuance of SSNs to non citizens if their immigration records have not been verified with the INS. This will likely result in delays that would previously have been thought unacceptable by SSA, but I applaud the Commissioner's resolve in making this stand.

With regard to the proposed enumeration centers, which would have the ability to recognize counterfeit documents, prevent the issuance of SSN cards to illegals, and conduct investigations, SSA advises me that they are not yet prepared to announce the rollout of this pilot project. The idea is that all U.S. citizens, not enumerated at birth, or foreign nationals who want an SSN would have to go to an enumeration center. There is a pilot being reviewed by SSA at this time.

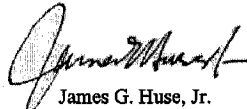
These SSA initiatives could delay the receipt of SSNs for some citizens and non citizens. However, they are necessary to ensure the integrity of the SSN and should help ensure that only those who should receive an SSN do so. SSA has been working closely with the States and INS to minimize possible delays. In a separate initiative, SSA is working with INS to issue SSNs to non citizens legally eligible for a number immediately upon entry into the U.S. This process would not be duplicative of the enumeration centers and if implemented successfully, should significantly reduce the number of individuals that SSA would have to enumerate.

Page 3 - The Honorable Sheila Jackson Lee

These initiatives will also make SSNs less accessible to people with criminal intent. We believe that they will deter individuals from using false or stolen birth records or immigration documents to obtain an SSN from SSA, and will help to ensure the integrity of the SSN for everyone.

I appreciate your strong interest in and commitment to the integrity of the SSN. If I can be of further assistance, please contact me or my Chief of Staff Richard A. Rohde at (202) 842-3613 extension 201.

Sincerely,



James G. Huse, Jr.  
Inspector General

PREPARED STATEMENT OF THE HONORABLE ZOE LOFGREN, A REPRESENTATIVE IN  
CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman. I regret that another previously scheduled commitment prevent me from remaining for the entire hearing. I appreciate the opportunity to review the thoughts of our witnesses before Attorney General Ashcroft and Homeland Security Director Tom Ridge testify before the Judiciary Committee this week.

There is no question that identity fraud and theft pose serious problems to US national security. While opportunities for identity theft have grown with the Internet, technology is ultimately also the answer.

I have long believed that the only real solution to identity theft and fraud lies with new developments in technology, and that the way to keep America secure is to ensure that our law enforcement and border protection agencies have the personnel and resources to quickly access and constantly update their technological resources.

For example, a social security card with a chip containing scanable bio-data is more secure than the piece of paper that my social security card is printed on. Iris scan technology is more secure than the current practice of fingerprinting. While developing and updating technology is an expensive proposition, a secure America is priceless.

On a more basic level, our law enforcement agencies must begin tracking identity theft and fraud. Since identity theft and fraudulent documents can be part of a larger serious crime or scheme, it makes sense to do more than compile statistics on these offenses.

I thank the witnesses for their testimony.

**Identity Theft Resource Center**  
PO Box 26833, San Diego CA 92196  
[www.idtheftcenter.org](http://www.idtheftcenter.org)  
email: [voices123@att.net](mailto:voices123@att.net)  
858-693-7935

**“The Risk to Homeland Security from Identity Fraud and Identity Theft”**

**June 25, 2002**

**Testimony for the joint hearing of the House Judiciary Subcommittees  
on Immigration, Border Security and Claims &  
Crime, Terrorism and Homeland Security**

Written Testimony Provided by:

Linda Foley, Executive Director, Identity Theft Resource Center (ITRC)

Members of the committee: Thank you for the opportunity to provide testimony for your committees today and for your interest in the topic of identity theft.

The Identity Theft Resource Center (ITRC) is a nonprofit program that was formed in December 1999 by Linda Foley, a victim of identity theft. It is an affiliated program of the Privacy Rights Clearinghouse, based in San Diego, California.

ITRC's mission is to research, analyze and distribute information about the growing crime of identity theft. It serves as a resource and advisory center for consumers, victims, law enforcement, legislators, businesses, media and governmental agencies. Specifically, our goals are to support victims of identity theft in self-advocacy, broaden consumer, corporate, governmental and legislative awareness and understanding of identity theft issues, and to decrease the potential victim population.

ITRC has learned much through its work with thousands of victims, members of law enforcement, governmental agencies and business. We hope to share some of what we have learned with you today.

Our written testimony is divided into five sections:

1. Identity theft and its impact on the nation
2. Misuse of the Social Security number (SSN) and the problem of information trafficking
3. ITRC's observations of the Social Security Administration's response to identity theft.
4. Misconceptions, in terms of identity theft, statistics and homeland security

## 5. Recommendations

### Part One: Identity theft and its potential impact on the nation

Through its interactions with district attorneys, members of law enforcement, business leaders and consumers, ITRC has concluded that as a nation we are underestimating the economic impact of identity theft. By applying economic models used to determine the potential affect of energy cost increases, it is possible to predict the impact of a large, organized identity theft crime. If properly orchestrated, it could significantly affect the nation's economy. We sincerely hope that would never happen, but no one expected planes to be used to destroy buildings either. Specific suggestions to reduce this risk will be included in the Recommendations section.

There is no single clearinghouse to report identity theft. Therefore, there is no central database of identity theft statistics. As a result, there are discrepancies in statistics about identity theft and this is part of the problem. However one conclusion is irrefutable. Identity theft is on the rise. For the purpose of this paper, ITRC will provide citations to the sources of statistics when possible and will concentrate on information provided by unbiased sources.

**Potential Economic Impact:** There are two sets of victims in identity theft: the consumer victim and the commercial victim. The following information demonstrates the potential impact on each.

#### Consumer Victim:

- 175-200 hours of lost time to repair damage done by imposter (PRC/CALPIRG)
- \$1,100+ in out-of-pocket expenses (FTC)
- Lost vacation or sick time (used to make phone calls, speak with law enforcement, pick up reports, fill out fraud affidavits, communicate with credit bureaus, travel to other jurisdictions, etc)
- Loss of productivity due to the distraction of the crime
- Emotional distress affecting job and interactions with family
- May have to pay higher mortgage or interest rates
- Immediate impact on purchasing power - unable to get credit, may lose job or be unable to get employment, unable to qualify for large ticket items, etc
- Extended diminished purchasing power: Delay in making large purchases affects commissions of those who would have sold the product to this victim which in turn leads to their diminished purchasing power (cyclic). Reduced purchasing affects businesses this person frequents in terms of loss income, may affect their ability to give raises, hire people, impacts layoffs, higher prices to make up for reduced sales that would normally have helped to pay for overhead. (cyclic)
- The loss of vacation time also impacts travel and hospitality industry due to cancellations



PRC: "Nowhere to Turn" - Privacy Rights Clearinghouse and CALPIRG (PRC/CALPIRG, May 2000), available at [www.privacyrights.org](http://www.privacyrights.org)  
 FTC: Federal Trade Commission, website info via [www.consumer.gov/sentinel](http://www.consumer.gov/sentinel)

The Commercial Victim - Merchants, credit issuers, financial institutions

A Florida Grand Jury recently impaneled to study the problem of identity theft concluded that the average loss to business was \$17,000 per victim. The PRC/CALPIRG study in 2000 (sourced above) concluded that the average loss per victim was \$18,000, with totals ranging from \$250 to \$200,000. For the purpose of this hearing, we did not use the FTC numbers since most of the reports they take are moment of discovery and cases frequently escalate as time goes on.

(Florida Report- Case No: SC 01-1095, First Interim Report Of The Sixteenth Statewide Grand Jury, January 10, 2002, available through ITRC website- [www.idtheftcenter.org](http://www.idtheftcenter.org), Speeches)

Experts estimate there were between 500,000 to 750,000 consumer victims last year alone. However, some members of law enforcement believe these numbers are low and place the count closer to one million. If you multiply the total number of victims and the cost to business the resulting potential loss in merchandise and services could exceed \$12 billion. Add to that loss the cost to victims, taxpayers (law enforcement, criminal justice, etc.) and consumers and you must conclude that identity theft cannot help but negatively impact the nation's economy.

In order to account for the loss businesses must:

- Increase prices = lessening customer purchasing power (leads to cycle) or
- Reduce staff hours or staff = lessens staff purchasing power (leads to cycle) or
- Absorb the loss which is economically unfeasible and an option that stock holders and insurance companies will not accept over the long run.

Secondary losses to businesses include:

- Fraud investigative time
- Loss of product to sell, restocking costs, paperwork, freight costs
- Loss of clientele who take their business to other companies that have adopted safer business practices in terms of identity theft and privacy issues
- Costs attributed to increased security measures and replacing computer programs with updated ones.
- Increased employee costs due to need to more thoroughly screen employees (both current and new), on-going training, etc.

#### **Part Two: Misuse of the Social Security number and the problem of Information Trafficking**

Since Inspector General James Huse. will be testifying, as well as someone from immigration, we will limit our discussion to issues about identity theft and not

assignment of SSNs to immigrants.

The problem of Social Security number (SSN) abuse and misuse (specific to identity theft) partially stems from an executive order issued by Franklin D. Roosevelt. This order allowed the SSN to be used for an extended number of purposes beyond the original intent. Unfortunately, it is difficult to unring this bell. Today it seems like every company and group would like to use to use this unique identifying number, ranging from health clubs to veterinarians. We have even heard that in some areas elementary school students must provide it to cafeteria workers to get their government-supported lunches. This leads to a proliferation of people with access to sensitive information.

Another part of the problem is that databases are not secure. The number of people who have access to SSNs via databases ranges in the millions. This is accentuated by the fact that most of us cannot even fathom how many lists include our numbers. What has resulted is a tremendous incidence of SSN information trafficking.

ITRC receives dozens of phone calls and emails every week from concerned consumers, companies and victims regarding SSN misuse and identity theft. The following list includes just a few of their concerns.

- **SSN use as military ID number:** The use of the SSN as a military identifier causes a great burden for the service person as well as his or her family. This number is imprinted on all belongings. This makes them especially vulnerable to workplace identity theft. Family members must carry ID cards in order to get on base, obtain medical care, and use the commissary, welfare and recreational facilities.

Lost and stolen wallets are a big problem area both for service people and family members since they are required to carry this ID card with them. Service people and families stationed abroad have an extremely difficult time connecting with credit reporting agencies and credit companies to close accounts, place fraud alerts, etc. They are also at higher risk of being targeted by information traffickers due to the accessibility of SSN via stolen wallets, databases and forms that may be viewed by non-classified personnel. These dedicated individuals put their lives on the line for us. The least we can do is to better protect them and their families by changing the military ID number back to a random serial number.

- **Elder endangerment:** A person's Medicare number is either his or her own SSN or that of the deceased spouse plus his or her own number along with it. Most seniors feel obligated to carry their cards at all times. This places them in a highly vulnerable position in regards to lost/stolen wallets (including muggings) as well as the problem of the high exposure of the SSN to health professionals and office staff.
- **SSN use as a health insurance number:** Many health insurance providers use the SSN as the provider number. This leads to problems with lost/stolen wallets and exposes the SSN to a large number of people and databases used for health-related purposes. One of our regional coordinators had her identity stolen because of a

prescription company database breach. Yet another had her identity stolen by the receptionist at her doctor's office.

- **SSN as a student ID number:** Once again, this is a situation of overexposure. Student numbers are used for registration, to purchase books, placed on roll sheets that are passed around the classroom, on grade cards (sometimes postcards sent via mail), and even included on lists posted on bulletin boards. Unfortunately FERPA does not seem to address all of these situations.
- **SSN of deceased:** Death does not stop information traffickers and identity thieves. Unfortunately the "Social Security Administration Master Death Registry" is not a master list at all. It is based on consumer-driven information, often including only those names involving a change in benefit status or request for death benefits. In order to be effective, there has to be a systematic reporting of every death to the SSA, the major credit reporting agencies and IRS. Each of these groups need to mark reported SSNs as "deceased" and flagged. ITRC has proposed such a bill for consideration (Gutierrez) which will be introduced later this year.
- **SSN of minors:** Today, babies are given SSN. There are three scenerios involving the SSN of minors. In the first, thieves use old newspaper archives and find death announcements for people about their own age (or who would now be their age) or depend on stealing information associated with children (ie. from a lost/stolen wallet). In the second, criminals watch for birth announcements and via the Internet or information traffickers purchase the SSNs to match. The third typically involves a relative or parent of the minor. In most cases, thieves end up with a large window of opportunity and the ability to do a lot of damage prior to being stopped. Sometimes the child doesn't find out about the theft until they apply for credit themselves or are denied a driver's license due to warrants and outstanding tickets. It's an excellent way for an identity clone to blend into our society.
- **SSN on public display:** Despite strong admonitions of the Office of the Inspector General, legislators, the Federal Trade Commission and consumer advocates, the SSN is still being used as a public identifier. Examples include driver's license numbers, employee numbers (including placement on badges, timecards, cash receipts, transaction records, paramedic reports by those firefighters who provided care), court records, police reports, professional licenses.
- **SSN as credit headers:** Credit headers are subject to purchase and accessible to those with "valid reasons to verify credit." Unfortunately, that means that information traffickers may list themselves as legitimate businesses and purchase these records. ITRC also is working with a number of women whose ex-husbands have been able to track them while posing as companies doing background checks.
- **Restrictions on companies or individuals requesting SSNs from individuals:**

Companies often ask for information that is not necessary for the transaction of business. They claim that they may need it at a future time or for statistical purposes. There should be some restriction of the type of information asked on applications. For example, a self-storage company and a health club were recently asked why they requested the person's SSN. The response was that it was a convenient ID number to use as a member number.

- Credit application verification: ITRC has been told that it is cheaper to "absorb costs associated with credit card fraud" than to verify applications. Senator Feinstein's S1399 (mandatory fraud alert program) must be approved and consumers must be given the ability to control when and how credit is extended.
- Computer security: In many cases, the concealment of computer breaches is a bigger problem than the breach itself. The seventh annual FBI Computer Security Study found only 36% of companies that experienced computer breaches reported them to law enforcement. Just last month, more than 260,000 California state employees were placed in financial jeopardy when their SSNs and database records were accessed by a hacker. The breach was not disclosed immediately upon discovery and California's Office of Privacy Protection (OPP) ([www.privacy.ca.gov](http://www.privacy.ca.gov)) is still evaluating how many people have become victims of financial fraud because of the delay. ITRC knows of several victims, though most are being directly by union officials to the OPP for assistance. (April 7, 2002. "Computer Crime and Security Survey," conducted by The Computer Security Institute with the participation of the San Francisco Federal Bureau of Investigation's Computer Intrusion Squad.)

**Part Three: ITRC's observations of the Social Security Administration's response to identity theft (based on victim testimonials to ITRC)**

1. Lack of response by SSA to reports of identity theft: When one's Social Security number has been abused it is almost instinctual to want to report this to the SSA. However, most victims say that they were unable to reach a live person and if they did, were discouraged from filing a report. Victims want to know if anyone else is reporting income under their SSN and to ask for their accounts to be flagged against possible fraud. The SSA appears to have taken a hands-off stance on fraudulent uses of the SSN. The problem seems to lie in the focus of what types of cases are being investigated, primarily benefit fraud. Customer service representatives have been quoted as saying, "The Social Security Administration issues numbers and administers benefits. It doesn't have any way of helping identity theft victims."
2. Problems with those who do change SSNs: When a person changes a SSN due to severe financial or criminal fraud, it is as if they have been reborn. In many ways this causes more problems than having an abused number attached to their identity. Victims report being unable to secure jobs, obtain credit, find rental housing, make major purchases, transfer college credits (or even access them as proof for a job), etc. Unfortunately many items are connected to the SSN and when a new number is issued, the individual loses their past. The SSA should have a standard procedure for helping these individuals transfer old credit, job and college information to the new

number without jeopardizing their identity. We have only had one person successfully do this himself. He is an attorney and it took several years of focused attention.

3. Correcting file errors: ITRC works with victims who have struggled to correct misinformation attached to their SSN. This may be due to mixed files, dual issue of SSN, identity theft or fraud, when an imposter works under another person's SSN, account/identity takeover, internal information trafficking, benefit fraud, etc. The biggest task victims face is connecting with an OIG investigator. Customer service personnel must be better trained on how to respond to "customers in crisis."

**Part Four: Misconceptions, in terms of identity theft, terrorism and homeland security**

1. Discrepancy in numbers: You will notice that the majority of the statistics we use are provided by independent sources and members of law enforcement. Part of that reason is that some members of the business community would have you believe that identity theft is much ado about nothing. This quote comes from American Banker (Friday, May 17, 2002, author Oscar Marquis)

*Much of the consumer angst about privacy is driven by the fear of becoming a victim of identity theft. As a result, new federal and state legislation is being introduced almost daily.*

*The resulting laws often create new obligations for financial institutions. The credit card number truncation laws passed by many states are one example. Credit file blocking is another.*

The question must be raised, why is the business community so intent on minimizing identity theft crime statistics? One reason might be that it costs money to truncate account numbers from receipts, honor fraud alerts, verify applications and redesign computer systems so that the Social Security number is not the primary identifier. Some in the business community view identity theft and the associated financial losses as trivial or minimal. While we see losses in the billions of dollars, they see an industry that is valued in the trillions. Their stance is that the recommended business practice will cost them more than the losses they now incur. ITRC believes that statistical information provided by business entities must be evaluated for intent and accuracy.

For example, a recent GAO study (March 2002 GAO-02-363) said that at least one credit reporting agency has concluded the only true ID theft victims they hear from are those that place 7-year alerts on credit reports. In our discussions with victims, most don't know that the alert they placed when originally calling for their report is a temporary one and that they must ask for the 7-year alert in writing. It should be noted that the CRAs bury that information in small print in the report and most people do not see it until it is pointed out to them. There are many reasons that people do not request a 7-year alert. Therefore, ITRC does not agree with the CRA and believes this is not a true measure of number of victims.

2. Need to reduce consumer privacy: Recent newspaper articles have brought attention that the fear of terrorism may be used to undermine consumer privacy. Unfortunately identity theft is often cited as a reason that consumers must give up more privacy. We strongly disagree with that concept and will address it further in Recommendations. This excerpt is from the Associated Press via Red Bluff Daily News, June 12, 2002, <http://www.redbluffdailynews.com>

*BANKS ASK GOVERNMENT TO BLOCK STATE PRIVACY LAWS  
By SHARON THEIMER-Associated Press Writer*

*WASHINGTON - The banking industry is reaching out to Homeland Security Director Tom Ridge and lawmakers in search of federal help to block state consumer privacy laws that bankers argue will hinder their efforts to spot terrorists.*

*Industry lobbyists have been arguing that state laws that prohibit banks from sharing consumer information without permission might preclude them from alerting law enforcement to potential crimes.*

*"We would have trouble communicating with law enforcement ... and it would be extremely chaotic. We need a uniform privacy standard," said David Liddle of the Financial Services Roundtable, an industry lobby.*

*Some state officials don't buy the argument, maintaining that state laws have adequate exemptions for law enforcement. They suggest the bankers are using national security to disguise their true intention of winning free rein to sell customer information for profit.*

*"What they ultimately want is the full use of the financial information of their customers for marketing purposes. This is about money," said North Dakota state Rep. Jim Kasper, a Republican who wants to toughen his state's privacy laws.*

3. National identity cards or driver's licenses: The argument against establishing either a national identity card or national driver's license was best stated in testimony provided to AAMVA (Feb. 10, 2002) by ACLU Asst. Director Barry Steinhardt "The Uniform Driver's License as a National ID." ([http://www.aclu.org/issues/privacy/AAMVA\\_Speech.html](http://www.aclu.org/issues/privacy/AAMVA_Speech.html)) Simply stated, neither a national identity card or driver's license is a protection against terrorism. The primary problem lies in the documentation used to secure these documents - birth certificates and Social Security cards. These breeder documents do not provide proof of identity. The birth certificate is only a record of a birth. The SS card is a card with a number and a name. Unfortunately, these documents are easily forged, bought and stolen. In fact, Mr. Huse testified in November that six of the hijackers obtained SSNs through fraudulent means. The adoption of a national card will only create a larger market for information trafficking and lull us into a false sense of security. Those who wish to obtain or create false documentation will always be able to do so. The only deterrent is to make it more difficult to get breeder documents and pass laws with stiff penalties against information trafficking. We also recommend that minimum standards be established for the securing of a driver's license, similar to the ones now used in California.

#### **Part Five: Recommendations**

1. Inclusion of financial fraud and identity theft case statistics in the FBI National Crime Index so that we have accurate, unbiased numbers defining the scope of this crime
2. Mandatory police reports: We desperately need to make sure that every financial fraud victim is able to make a report to law enforcement. Until we do so, we are all at risk. Federal legislation might state: "No state or local law enforcement agency shall refuse to take a crime report from an individual in their local jurisdiction who has learned or reasonably suspects that his or her personal identifying information, as defined by 18 USC 1028, has been unlawfully used by another and shall make a copy of said report available to the victim. If the suspected crime was committed in a different jurisdiction, the local agency may refer the matter to the law enforcement agency where the suspected crime was committed for an investigation of the facts. This law shall only set minimum requirements and not supersede a state law that holds law enforcement to a higher level of service."
3. Development of an ongoing committee composed of consumer groups, FTC and law enforcement agencies to continue the exploration of homeland security and identity theft. Since this is an evolving problem, and the criminal element is continually finding new ways to steal and use identities, it is important to discuss trends and ways to fight them. The FTC identity theft program staff is already overworked and cannot expect to do this job on their own.
4. Development of an investigative law enforcement taskforce - composed of members from the FBI, Secret Service, U.S. Post Office, Immigration Services (INS), IRS, AAMVA, U.S. Attorney General's Office, Office Of Inspector General (SSA), military JAG, fraud investigators from each of the major credit reporting agencies, VISA and Mastercard, and from each state - at least one state marshall, one Department of Motor Vehicle investigator and one state attorney general. This could be funded by Homeland Security and could actually save money due to the elimination of duplicated efforts.

Since we know that identity theft and financial crimes often cross jurisdiction lines, both geographic and departmental, a multi-agency group would open doors of communication and avoid expensive replication. By combining the intelligence and resources of these agencies, this task force is in the position to recognize trends, spot and stop new crime ring activity, coordinate and connect apparently unrelated cases into larger cases (most imposters attack numerous victims simultaneously), investigate large cases of information trafficking or workplace identity theft and effectively work with the victims of these crimes. They would also be an ad hoc group advising Homeland Security and coordinating efforts to spot and stop terrorists.

This unit should also establish criteria for local case referral. For example, one criteria might be a situation where a victim finds out that another person is also reporting income as them. However, the two jobs might be physically impossible to do simultaneously either due to time constraints or geographic distance.

5. Victims of financial fraud must be given full rights under the law. These include the right to reasonable and timely notice of any public proceeding involving the crime and of any release or escape of the accused; the rights not to be excluded from such public proceeding and reasonably to be heard at public release, plea, sentencing, reprieve, and pardon proceedings; and the right to adjudicative decisions that duly consider the victim's safety, interest in avoiding unreasonable delay, and just and timely claims to restitution from the offender.
6. We must phase out the use of the SSN as a military ID and Medicare number: Both of these groups are required to carry cards that contain the SSN and provide these numbers frequently. If it is deemed that the program cannot be changed, at least we must consider assigning a random public number to each person that links to the SSN in a database program. While database breaches do occur, at least this would minimize public exposure of SSNs for these two vulnerable groups. The phase out of these numbers can be done over several years to minimize costs.
7. New standards and laws need to be adopted that dictate collection, use, display, security and confidentiality of the SSN. It should not be used as an identifier by schools, insurance companies, employers, utility companies or businesses. SSNs should not be publically displayed (ie. printed on timecards or badges) or shared with other companies or organizations except where required by law. Penalties need to be imposed on those who do not comply with these standards. Again, a phase out program can be implemented to minimize costs to those entities that now use the SSN as the customer ID number. An example of such a program can be found in the California Civil Code Section 1798.85 (passed 2001- SB 168). The law, which begins to take effect in July 2001 and must be fully effective by no later than July 2005, applies to individuals and non-governmental entities. Under the law's provisions, companies may not do any of the following:
  - post or publicly display SSNs
  - print SSNs on identification cards or badges
  - require people to transmit an SSN over the Internet unless the connection is secure or the number is encrypted
  - require people to log onto a web site using an SSN without a password
  - print SSNs on anything mailed to a customer unless required by law or the document is a form or application

The law has a phased-in compliance schedule.
8. Congress must pass laws that give credit issuers an incentive to check credit applications more carefully. There should be effective disincentives, such as monetary penalties, for those credit issuers who rely solely on the SSN when granting credit. "Credit issuers" include credit card companies, loan issuers and companies (auto, home), phone and electricity utility companies, etc.
9. Computer security: The concealment and notification delay to concerned parties of computer breaches involving the theft or possible theft of identifying information



must stop. Legislation needs to be considered (ie. Calif. SB 1386, 2002 leg. session, [www.leginfo.ca.gov](http://www.leginfo.ca.gov)) that would require a timely notification to all parties involved in a computer breach containing their personal identifying information.

We of the Identity Theft Resource Center thank you for your time and consideration of this topic. Identity theft can be devastating and we have noticed that the "worse-case scenerios" seem to be getting worse than months prior. ITRC would love to be put "out of business" but don't see that happening anytime soon. As it is, the number of victims who contact us for help is constantly increasing.

Please feel free to contact us with any questions. We urge you to take steps quickly. There are many people who truly understand this crime. We don't need more studies; we need to become more active - both proactive in crime prevention and reactive in solving crimes and helping victims.

Sincerely,

Linda Foley  
Executive Director,  
Identity Theft Resource Center

Children Taken Away From Identity Theft Victim SACRAMENTO, Calif., 9:36 a.m.  
 PDT April 24, 2002 - Victims of identity theft often lose money or property. But for one day, one Northern California woman lost something much more important -- her children.

Earlier this year, someone stole Sacramento resident Angela Johnson's purse and eventually her identity. On Sunday, a pregnant woman checked into Mercy General Hospital with Johnson's I.D. and gave birth. The woman disappeared. Doctors later determined that the baby was sick because the mother used "crack." So hospital officials gave her name to Child Protective Services. The name was Angela Johnson. CPS workers put the older child into protective custody and took her to the younger one's day car center, thinking Johnson was the one who gave birth at the hospital. Johnson said that when she asked where her children were, CPS would not tell her. The problem is that the real Angela Johnson had done nothing wrong. She was just the victim of identity theft. Johnson said that it took several humiliating hours to get her children back. CPS said that the blame ultimately lies with the person who deceived everyone. "The hospital was a victim of identity theft. We were victims. And this mother was a victim. And I'm sorry for all of us," CPS spokesman Jim Hunt said. "I felt that it was the opposite way. That we were guilty until proven innocent," Johnson said.

**We submit these media articles for consideration as well.**

This From: Sacramento Bee, June 13, 2002

#### **Colleges illegally use Social Security numbers**

Three Los Rios schools use them to post grades around the campuses.

<http://www.sacbee.com/content/news/story/3192794p-4241429c.html> By Terri Hardy -- Bee Staff Writer

Sacramento community colleges that long have posted grades around campus by referring to the last four digits of students' Social Security numbers were unknowingly violating federal privacy law.

The 1974 Family Educational Rights and Privacy Act forbids using even a portion of the Social Security number when listing grades, said Jim Bradshaw, a spokesman for the U.S. Department of Education.

"The act prevents information from being disclosed that is personally identifiable," Bradshaw said.

"If you happen to have someone's Social Security number or a portion of that number, it's possible to get information on a student they might not want you to obtain."

The question about the use of Social Security numbers was raised when a visitor familiar with federal privacy laws recently noticed grades posted on windows at a local college. Officials at Cosumnes River, American River and Sacramento City colleges say that teachers for years have publicly posted grades on campus by using the last part of students' Social Security numbers.

They said they never realized the practice violated the law and considered the postings a courtesy for anxious students who didn't want to wait for their grades in the mail.

"It's such a common practice, probably all of education uses Social Security numbers (when posting grades)," said Susie Williams, spokeswoman for the Los Rios Community College District, which includes the three campuses. "It's about ease. It's a number everybody knows, that everybody has."

Williams said the district is phasing in a new software program that will let it issue new student ID numbers, so it will no longer use Social Security numbers to publicly list grades.

Ralph Black, general counsel for the California Community Colleges chancellor's office, said it is a privacy violation to post portions of Social Security numbers. He said he doesn't know how common the practice is at other community colleges.

"We don't directly control how districts deal with the use of Social Security numbers, but we do advise them if they call us and request our advice," Black said.

Officials from the University of California, Davis, said campus policy lets instructors post grades using a student's full Social Security number, if the student provides written consent. They believe they are allowed to use a portion of the Social Security number without written permission. But since 2000, UC Davis has moved away from using Social Security numbers as personal identifiers for students as well as employees.

"We now have the technology to create new numbers," said Jeanne Wilson, coordinator for student-related policy development and compliance. "There's been a lot of national attention on Social Security numbers, but I'm not aware of anything from the (Education Department) that said using even a portion of the number is a problem."

California State University, Sacramento, discourages teachers from using Social Security numbers to list grades, said Ann Reed, campus spokeswoman. "Do they occasionally violate that? Probably," she said.

In a campuswide memo in December, CSUS officials warned that a Social Security number is never to be released. "For example, class rosters may not be posted to report exam or final grades," the memo said. "Documents showing (Social Security numbers) must be disposed of by shredding or burning."

Reed said there's no reason to post grades publicly now because they can be accessed through telephone or computer using a personal identification number.

The U.S. Department of Education occasionally learns that colleges are violating the privacy act when they display Social Security numbers, Bradshaw said. He said the department has tried to get the word out, and he believes more campuses are aware the practice is illegal.